KOBIL mIDentity V1.5.2
User Manual

16.07.2007
English Version

Contents

1 What is KOBIL mIDentity? 2
- 1.1 Content . . . 2
- 1.2 System Requirements . . . 2

2 Getting started with KOBIL mIDentity 3
- 2.1 Insert your KOBIL mIDentity SmartCard . . . 3
- 2.2 KOBIL mIDentity Software Installation . . . 5
- 2.3 Entering the License Key . . . 7

3 First Steps 10
- 3.1 Your personal KOBIL mIDentity . . . 10
- 3.2 Remove KOBIL mIDentity securely . . . 11
- 3.3 The KOBIL mIDentity SmartCard . . . 11
  - 3.3.1 Initialization of the SmartCard . . . 12
  - 3.3.2 Specifics of an T-TeleSec E4 NetKey Card from T-Systems . . . 16
  - 3.3.3 What happens if I enter the wrong PIN? . . . 17
  - 3.3.4 Change / Unlock the KOBIL mIDentity SmartCard PIN . . . 17
- 3.4 Digital Certificates . . . 18
  - 3.4.1 What is a Digital Certificate? . . . 19
  - 3.4.2 Where do I get my digital certificate from? . . . 19
  - 3.4.3 The Windows Certificate Manager . . . 21
  - 3.4.4 Importing a Trust Centre (CA) Certificate . . . 23
  - 3.4.5 Importing another User's Certificate . . . 24
  - 3.4.6 Import an existing certificate onto the KOBIL mIDentity SmartCard . . . 25
  - 3.4.7 Replace current SSO and Secure Data Storage certificate . . . 27
  - 3.4.8 Delete certificates from your KOBIL mIDentity SmartCard . . . 30
- 3.5 KOBIL mIDentity Personalization . . . 31
- 3.6 Software Updates . . . 31

4 Your mobile Identity 32
- 4.1 Passwords and Simple Sign-On (SSO) . . . 32
  - 4.1.1 What is Simple Sign-On (SSO)? . . . 32
  - 4.1.2 Using Simple Sign-On - Survey . . . 33
  - 4.1.3 Learning Passwords . . . 37
  - 4.1.4 Working with Console Applications . . . 43
  - 4.1.5 Managing Logon Accounts . . . 46
  - 4.1.6 Backup Logon Accounts (Simple Sign-On . . . 49
  - 4.1.7 Restore Logon Accounts . . . 51
  - 4.1.8 KOBIL mIDentity SSO Emergency Assistant . . . 53
- 4.2 Windows SmartCard Logon . . . 56

5 Your mobile Secure Data Storage **58**
5.1 Strong Encryption for sensitive Data . . . 58
5.2 Secure Data Storages with KOBIL mIDentity . . . 58
5.2.1 Creating a Secure Data Storage on your local hard disk . . . 59
5.2.2 Creating a Secure Data Storage on your network drive . . . 61
5.2.3 Creating a mobile Secure Data Storage on KOBIL mIDentity . . . 62
5.2.4 Working with Secure Data Storages . . . 64
5.2.5 Delete Secure Data Storages . . . 64
5.2.6 Delete a link to a Secure Data Storage . . . 65
5.3 File Security . . . 67
5.3.1 File and Directory Encryption . . . 67
5.3.2 Add/Remove encryption Recipients . . . 70
5.3.3 File and Directory Decryption . . . 70
5.3.4 File and Directory Signature . . . 72
5.3.5 Multiple Signatures . . . 74
5.3.6 File and Directory Signature Verification . . . 74
5.3.7 Signature and Encryption of Files and Directories . . . 76
5.3.8 Signature Verification and Decryption of Files and Directories . . . 79
5.3.9 Default Settings for File Security . . . 80
5.4 Emergency Recovery . . . 84
5.4.1 Additional Decryption Keys . . . 84

6 Your mobile Office **85**
6.1 Secure Email Communication using Outlook & Outlook Express . . . 85
6.1.1 Configure your Certificate . . . 85
6.1.2 Setting up Outlook Security Buttons . . . 91
6.1.3 Sending secure Email . . . 91
6.1.4 Receiving secure E-mail . . . 94
6.2 KOBIL eSecure für SAP R3 . . . 95

A Cryptographic Basics and Standards **96**
A.1 Security Objectives . . . 96
A.2 Terms and Basics . . . 96
A.3 Standards . . . 97
A.3.1 Data Digestion Algorithms . . . 97
A.3.2 Symmetric Encryption Algorithms . . . 97
A.3.3 Public Key Algorithms . . . 98
A.3.4 Digital Certificates . . . 103
A.3.5 Certificate Authorities . . . 104
A.3.6 SmartCards and Readers . . . 105
A.3.7 Secure Socket Layer (SSL) . . . 105
A.3.8 Secure Multipurpose Internet Mail Exchange (S/MIME) . . . 106

B Glossary **109**

Chapter 1

What is KOBIL mIDentity?

KOBIL mIDentity is a completely new product which will help you to simplify your life. No matter if you are in the office, on the road or at home: KOBIL mIDentity makes your world mobile since it is your mobile Identity, your mobile Datasafe and your mobile Office.

1.1 Content

- KOBIL mIDentity Light / Basic / Classic
- Key Ring
- (optional) Docking Station with 1.8m USB 2.0 cable
- (optional) SIM-sized Smart Card
- (optional) CD-ROM
- (optional) License-Key (only KOBIL mIDentity Light+)

1.2 System Requirements

- Operating Systems:
  Microsoft Windows 2000 (min. Service Pack 3) or
  Microsoft Windows XP (min. Service Pack 1) or
  Microsoft Windows 2000/2003 Server[1]
- Supported Software:
  Microsoft Internet Explorer 5.5
  Microsoft Outlook from version 2000 SR-1 or
  Microsoft Office from version 2000
- Hardware:
  256 MB RAM
  20 MB free Hard Disk space
  A free USB-1.1 or USB 2.0 port

[1] please find special Server-Setup on CD

Chapter 2

Getting started with KOBIL mIDentity

2.1 Insert your KOBIL mIDentity SmartCard

Together with your KOBIL mIDentity, you receive a SIM-sized SmartCard which is either shipped together with KOBIL mIDentity or seperately handed out from your system administrator. You have to break out the SmartCard (similar to mobile phones) and insert it into KOBIL mIDentity.

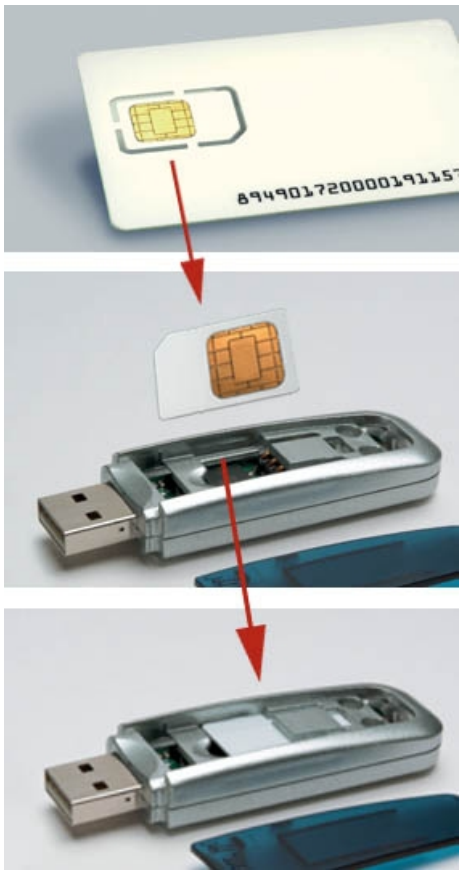

Figure 2.1: Insert the KOBIL mIDentity SmartCard

Note: Please remove the KOBIL mIDentity SmartCard only when KOBIL mIDentity is NOT plugged into the computer's USB port. Use the lit cover in order to simplify SmartCard remove.

Figure 2.2: Remove the SmartCard from KOBIL mIDentity

2.2 KOBIL mIDentity Software Installation

The KOBIL mIDentity software can be used for all mIDentity models and either is shipped together with the KOBIL mIDentity package on a CD-ROM or you can download the most recent version in the internet under http://www.kobil.com/mIDentity. Take a look here from time to time to see if new updates are available.

1. Start your PC
   Note: Please make sure that your KOBIL mIDentity is not plugged in while the software setup is running!
2. Make sure that you are logged in as **Administrator** (only needed for installation)
3. Finish all running programs.
4. Insert the KOBIL mIDentity Software CD-ROM into your CD-ROM/DVD-ROM drive, the setup will start automatically. If this is not the case, please start it manually using the Windows Explorer and select the menu item KOBIL mIDentity Software Installation.
   If you dont have any KOBIL mIDentity Software CD-ROM at hand, you can download the most recent version in the internet under http://www.kobil.com/mIDentity and start it by a double click.
5. Choose the installation language and click on OK

Wählen Sie eine Setup-Sprache aus
Wählen Sie die Sprache dieser Installation aus der unten aufgeführten Auswahl aus.
Deutsch
Deutsch
Englisch

Figure 2.3: Choose the installation language

6. Please read carefully the licence agreement. If you agree with it, click Yes in order to continue the installation process. If you dont agree, please click No to cancel the software installation.

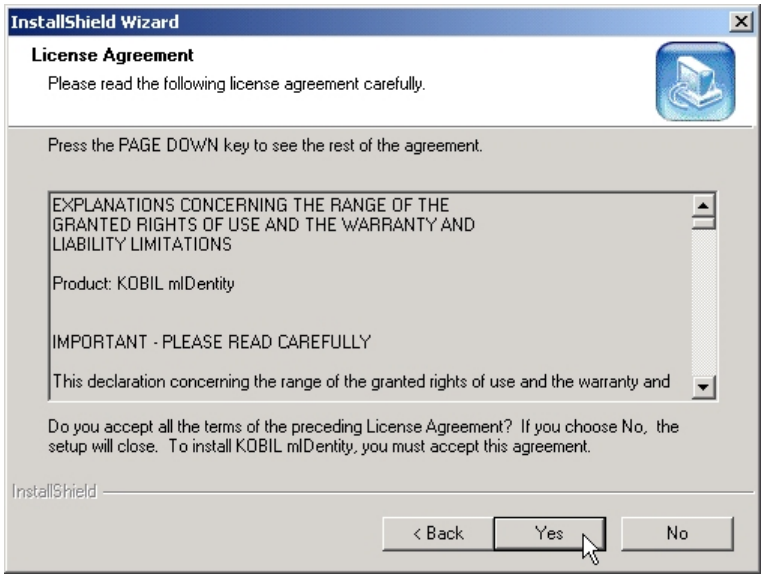
InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
Press the PAGE DOWN key to see the rest of the agreement.
EXPLANATIONS CONCERNING THE RANGE OF THE
GRANTED RIGHTS OF USE AND THE WARRANTY AND
LIABILITY LIMITATIONS
Product: KOBIL mIDentity
IMPORTANT - PLEASE READ CAREFULLY
This declaration concerning the range of the granted rights of use and the warranty and
Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install KOBIL mIDentity, you must accept this agreement.
InstallShield
< Back
Yes
No

Figure 2.4: Accept the Licence Agreement

7. Now you will be asked to define the installation folder for the KOBIL mIDentity Software. Usually, you can use the default values and just click on Continue to start the installation.

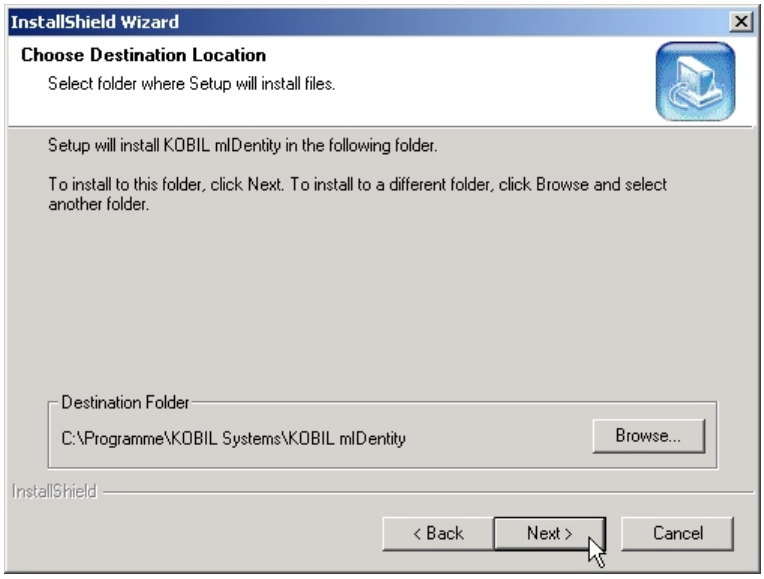
InstallShield Wizard
Choose Destination Location
Select folder where Setup will install files.
Setup will install KOBIL mIDentity in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\Programme\KOBIL Systems\KOBIL mIDentity
Browse...
InstallShield
< Back
Next >
Cancel

Figure 2.5: Installation Path selection

8. In the last dialog box, click Finish to complete the installation.

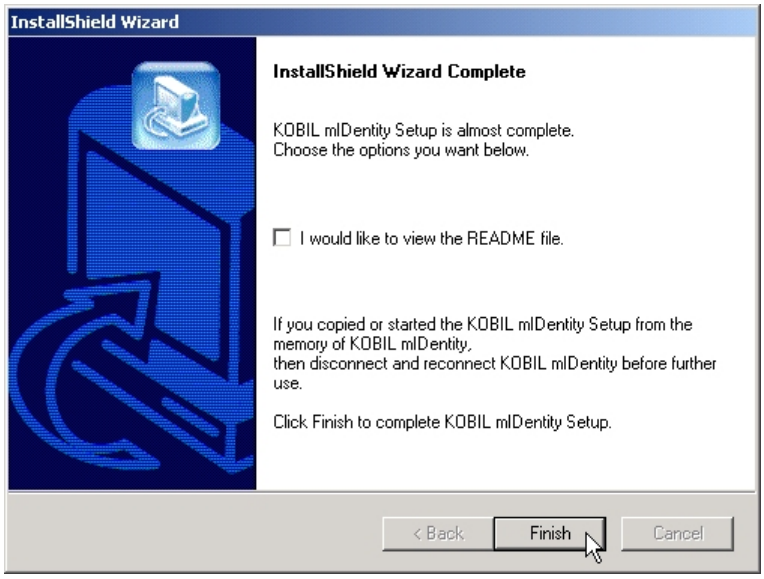
InstallShield Wizard
InstallShield Wizard Complete
KOBIL mIDentity Setup is almost complete.
Choose the options you want below.
I would like to view the README file.
If you copied or started the KOBIL mIDentity Setup from the memory of KOBIL mIDentity,
then disconnect and reconnect KOBIL mIDentity before further use.
Click Finish to complete KOBIL mIDentity Setup.
< Back
Finish
Cancel

Figure 2.6: Complete the Installation

Note: Before using the KOBIL mIDentity Software for the first time, please take a look into the installed user manual as well as the release notes to get the latest product information.

After successful installation, please double click the KOBIL mIDentity icon on your computers desktop to start the KOBIL mIDentity Software. The software runs in the Windows Tray Bar (at the right bottom next to the system clock). You can right-click on this icon to open the fast-access menu or perform a double click to open the main window.

2.3 Entering the License Key

As long as no KOBIL mIDentity device is plugged in, all functionality (except the user manual) is disabled. Depending on the KOBIL mIDentity package you have purchased, not all functions of the software are enabled after inserting the device. If you are using KOBIL mIDentity Light+ or KOBIL mIDentity Basic + upgrade, further functionality may be enabled by entering a license key. A message box with the neccessary information will appear when you plug in your KOBIL mIDentity device for the first time. This license key is either shipped together with your KOBIL mIDentity package (if you have purchased the full software features) or you can purchase it later as an upgrade at your certified KOBIL partner.

Following packages can be purchased:

- KOBIL mIDentity Light: Key request while using the software for the first time can be ignored (cancel request).
- KOBIL mIDentity Light+: Enter the license key which was shipped together with your KOBIL mIDentity package

when using the software for the first time. How to enter this key later, see beneath this section.

- KOBIL mIDentity Basic: Key request while using the software for the first time can be ignored (cancel request). To enable the full functionality enter the key which is shipped together with your upgrade as described beneath this section.

- KOBIL mIDentity Classic: Full functionality without any request.

To enter your license key, please select Settings Other Info and enter the license key into the appropriate text fields.

Miscellaneous
Info
PIN caching
File security
At the moment you use the following hardware:
KOBIL Systems KAAN SIM III 1 / 8949017200002717723
and the following software
KOBIL mIDentity V1.5 MSDI Build : 20050914.1
Click
www.kobil.com/mIDentity
to search for newer versions.
KOBIL mIDentity Software-License
Depending on your KOBIL mIDentity package, you have to enter a valid license key in order to use the full KOBIL mIDentity functionality. This key is either shipped together with the package or you can purchase it from your certified KOBIL partner.
Klick on "Enter License Key..." to enter the license key now.
Enter License Key ...
www.kobil.com/mIDentity
Close

Figure 2.7: Entering the License Key

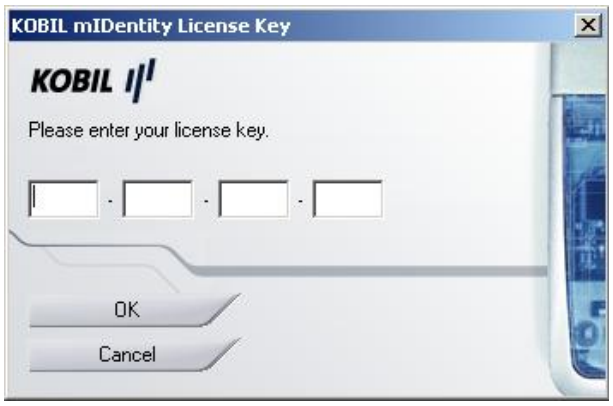

Figure 2.8: Entering the License Key

Chapter 3

First Steps

3.1 Your personal KOBIL mIDentity

The KOBIL mIDentity Control Centre Software consists of a main window (see figure 3.1) and a traybar menu which resides in the Windows Tray Bar at the right bottom near the system clock (see figure 3.2).

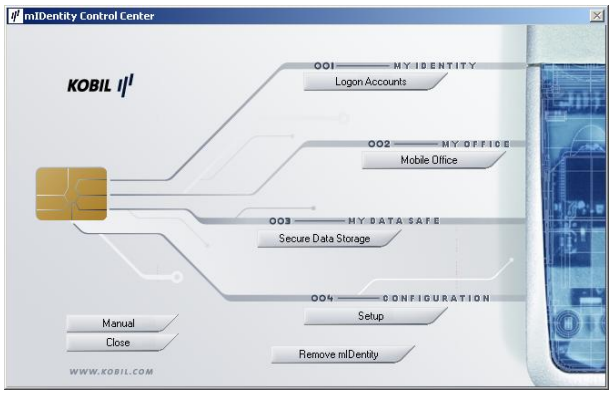

Figure 3.1: KOBIL mIDentity Control Centre main window

By double-clicking the tray bar icon, the main window is opened. All functions can be used by both the main window and the tray bar menu. The main window is better for untrained users while the tray bar menu allows fast work for power users.

Figure 3.2: Tray Bar Menu

3.2 Remove KOBIL mIDentity securely

Important! If you want to unplug KOBIL mIDentity, you have to use the secure remove function first to avoid data loss! This is also necessary on Windows XP and 2003 to close any open datasafe.

Right-click on the tray bar menu (see figure 3.3) and select **remove mIDentity**. Alternatively, you can click on the button **remove mIDentity** in the main window.

Figure 3.3: remove KOBIL mIDentity securely

3.3 The KOBIL mIDentity SmartCard

The KOBIL mIDentity SmartCard is KOBIL mIDentity's secure core, since it stores your personal information and keys securely. Without the SmartCard, no access to secured data is possible. All KOBIL mIDentity functions are protected by the KOBIL mIDentity SmartCard's PIN (personal identification number). As only you know the PIN, nobody else can use the functions or access secured data. The PIN is protected by a **failure counter** that locks the SmartCard after three subsequent wrong PIN entries. Only by entering the PUK (PIN Unblocking Code), the PIN can be unlocked (similar to mobile phones). You get your PIN either together with the KOBIL mIDentity SmartCard from your system administrator or - if the SmartCard is still empty - you can set the initial PIN and PUK at the first usage of KOBIL mIDentity. Please remember PIN and PUK very well since without them, you cannot use KOBIL mIDentity!

3.3.1 Initialization of the SmartCard

Once the KOBIL mIDentity setup software have been installed on your PC (see section 2), you can use the device. Start the KOBIL mIDentity Control Centre application and plug KOBIL mIDentity into the docking station or directly to an USB port on your PC.

If your KOBIL mIDentity SmartCard has already been initialized, i.e. PIN, PUK and an encryption certificate were defined, then you can proceed with entering the PIN number to access the card storage.
If your SmartCard is empty, which means PIN, PUK and an encryption certificate are not defined, the KOBIL mIDentity Installation Wizard will guide you through KOBIL mIDentity installation procedure. The Wizard will appear on your PC screen.
The very first screen of the Installation Wizard shows SmartCards current status. (see figure3.4). Follow the instructions on screens to complete installation.

Figure 3.4: KOBIL mIDentity initialisation-assistant (empty card)

1. Set up PIN and PUK:
   PIN (Personal Identification Number) is used to access the KOBIL mIDentity storage. You can choose your own PIN as a combination of 6-16 alphanumeric characters.
   PUK (PIN Unblocking Code) is used to unlock a locked PIN. You can define your own PUK or ask the system to generate a PUK for you. The PUK must be a combination of 6-16 alphanumeric characters.
   It is recommended to choose the system-generated PUK option, since human-created character sequences tend to be highly predictable (e.g. birthday). Make sure you print the generated PUK and save it in a secure place. (see figure3.5).

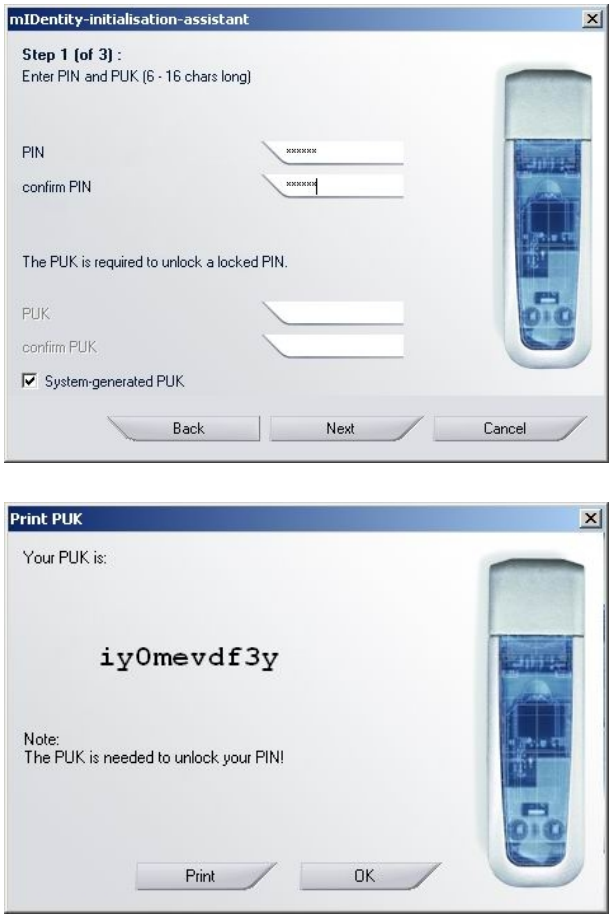

Figure 3.5: Set up PIN and PUK / show and print the PUK

2. Create a certificate for encryption:
   To encrypt data you require a certificate. You can create your own certificate (in PKCS#7 format) or import a certificate (in PKCS#12 format) from your PC. This certificate will be used to encrypt data in your Safe Data Storages and also to encrypt all your application access (logon) dialogs, containing your user ids and passwords.
   You can also define an Additional Decryption Key (ADK) for even better data protection. (ADK - see section 5.4).

Figure 3.6: create a selfsigned certificate

If you choose to create a certificate and use it for email signature, you will be asked to fill out some personal information.

Figure 3.7: create an own certificate

3. Assign a certificate for secure data storages and logon accounts (Simple Sign-On):
   If you choose not to create your own certificate but to import one, you will be given a list of certificates present on your PC to select the one you want to use.

Figure 3.8: Assign certificates

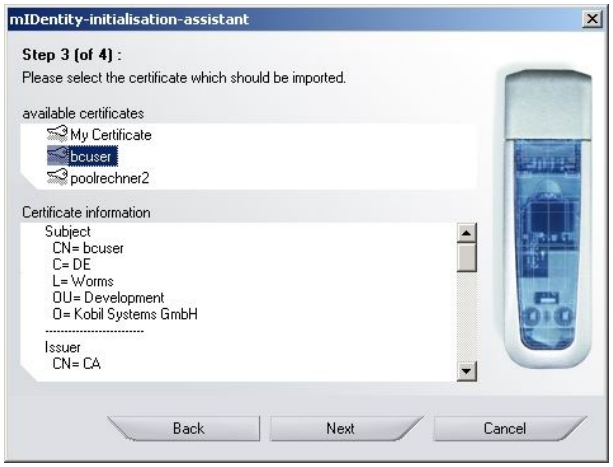

Figure 3.9: Select a certificate

As a final step of the initialization, the Wizard will display the current KOBIL mIDentity setup status.

Figure 3.10: Finish screen

3.3.2 Specifics of an T-TeleSec E4 NetKey Card from T-Systems

Some of KOBIL mIDentity supported SmartCard's has a different behavior in delivery status. The E4 NetKey Card is shipped in a transport- or null-PIN-state. This means after you reciept the card the PIN is already set. A transport- or null-PIN is a six digit long PIN, with all digits set to zero. When using this card for the first time, you have to change the PIN to an individual PIN which can be choosen by yourself.

A further specific is a so-called ePUK. ePUK means a PUK which is calculated automaticly while manufacturing and stored direct on the card. To obtain the ePUK, you have to enter your PIN and then you can read out the ePUK.

Initialization of an E4 NetKey Card

If you insert KOBIL mIDentity within an E4 NetKey Card for the first time, the KOBIL mIDentity Control Centre software will automaticly detect whether this card is in a transport- or null-PIN-state or not. If the card is in such a state, you will be asked to enter your new PIN twice. Additionaly you can read out or print out your ePUK. If you don't remember your ePUK after this initialization process, you can read out the ePUK later as well. Just click under

Preferences > Identity > mIDentity Smart Card

the button **read ePUK**. You will be asked for your PIN to read out the ePUK. Additionaly, you can print out your ePUK. Both buttons are only active if the inserted smart card is an E4 NetKey Card. The knowledge about your ePUK is specially important if you need to unblock the PIN (please refer to 3.3.4).

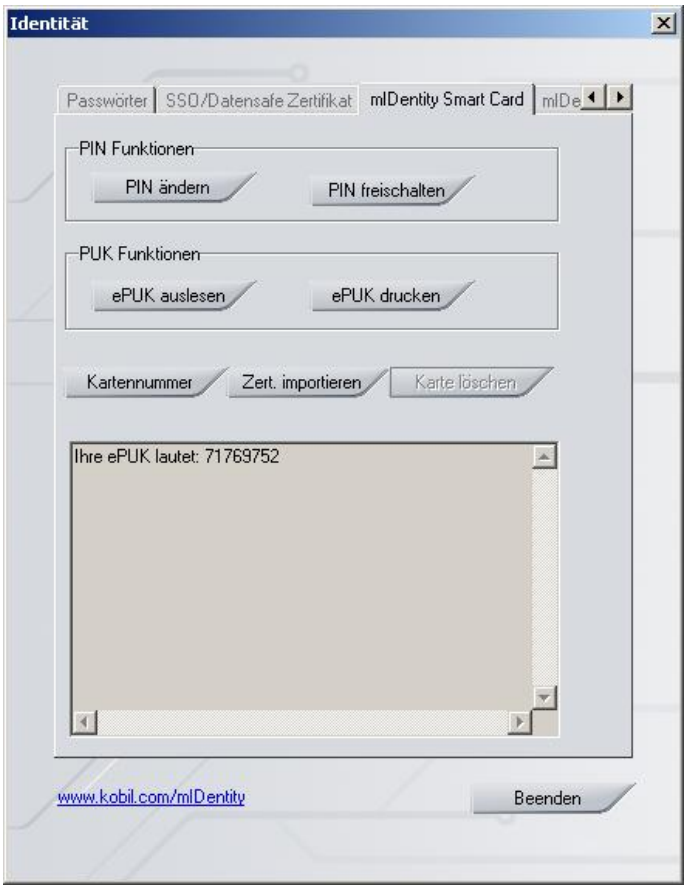

Figure 3.11: KOBIL mIDentity SmartCard preferences - ePUK reading/printing

IMPORTANT: If you print out your ePUK please take care that nobody has access to your secret data!

3.3.3 What happens if I enter the wrong PIN?

If you have entered the wrong PIN three times subsequently, the KOBIL mIDentity SmartCard is locked in order to protect access to KOBIL mIDentity for unauthorized persons. If you entered a wrong PIN, please take care to enter the correct PIN the next time. Once the PIN is locked, it can be unlocked by entering the PUK - similar to mobile phones (see section 3.3.4).

If a wrong PUK is entered three times, the SmartCard is irreversibly locked. In this case you should replace it by a new SmartCard which can be ordered at your local KOBIL dealer. If you have encrypted data on your hard disk (files or datasafe's), please read section 5.4 to learn how to recover them.

3.3.4 Change / Unlock the KOBIL mIDentity SmartCard PIN

You can can change and unlock the SmartCard PIN using the preferences in the Control Centre software. Please choose the option

Properties... > Identity

and select the drawer **Card** and click on **Change PIN**. You will be asked to enter the old PIN followed by the new PIN which has to be entered twice to avoid mistyping.

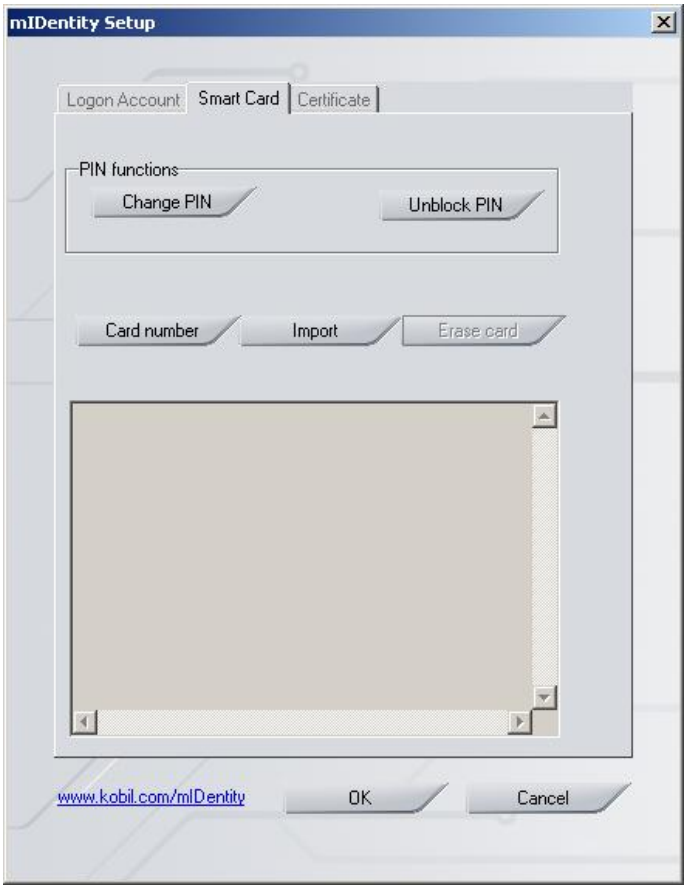

Figure 3.12: KOBIL mIDentity SmartCard preferences - change/unlock PIN

If KOBIL mIDentity SmartCard's PIN is locked (because you have entered a wrong PIN too many times), you can unlock it using the PUK (PIN Unblocking Code) as you may know it from your mobile phone. Click on **Unlock PIN** and enter the PUK, followed by the new PIN.

3.4 Digital Certificates

Your KOBIL mIDentity SmartCard can do much more than store only passwords and Simple Sign-On parameters. It is a full-fledged cryptographic SmartCard that can also operate with digital certificates and public key infrastructures (PKI technology). In this section, you learn what a digital certificate is, how you can obtain it and what you can do with it.

3.4.1 What is a Digital Certificate?

Digital Certificates are electronic ID-cards, you can use them as a digital identity. This makes much sense in networks and in the internet, because you cannot see your communications partners "face-to-face".

Exactly as in your real ID-card, a digital certificate contains your name and maybe some other informations about you and about usage constraints, e.g. network logon, encryption, signatures. For more details about digital certificates, see section A.3.4.

There is also a special kind of certificates, the so-called **Selbf-Signed Certificates**. These certificates are not issued by a trust centre. Everybody can create them, they work completely without any PKI infrastructure. This is why they are very easy to use, but of course they offer a lower level of identification compared with real trust centre certificates.

Self-signed certificates are used by KOBIL mIDentity to encrypt datasafes where they are no security risk since they are not used for communication with other people, but only for access to local and mobile datasafes (see section 5.2). Furthermore, they can be used for a simple file encryption.

3.4.2 Where do I get my digital certificate from?

There are many ways to obtain your personal certificate on KOBIL mIDentity which are suitable for different applications scenarios. Here you find an overview of them:

Self-signed Certificates

The fastest way to your self-signed certificate is about datasafes, since a self-signed certificate is automatically created as soon as you create your first datasafe. You recognize it by its serial number in the Windows Certificate Manager, for example **894917200000000026481**. You can watch it in the KOBIL mIDentity preferences on the **certificates** drawer.

Running your own trust centre

If you want to create your own public key infrastructure (PKI), you have to run a trust centre.

The corresponding software comes for example with Windows 2000 or 2003 Server (see also section 4.2). You can also buy specialized PKI server solutions, for example the KOBIL mIDentity Manager that can be configured to specific environments and requirements.

External trust centres

You can store also certificates from third-party trust centres on KOBIL mIDentity. Proceed as follows:

1. Start Internet Explorer
2. Surf to your preferred trust centre's URL, for example:
   TeleSec - trust centre (Germany): www.telesec.de
   TC trust centre (Germany): www.trustcenter.de
   Verisign (USA): www.verisign.com
3. Most trust centres offer free test certificates, also called *Digital ID's*. Please note that those test certificates do not offer a high security level since users are not identified very deeply.

4. Now you have to enter some data which will occur later in your certificate (parameters vary between trust centres). In most cases these are some personal data as well as your email address.
   It is extremly important that you enter your exact email address (case-sensitive) if you want to use that certificate for secure email!

5. When asked for the CSP to generate the keys, please select **Kobil Smart CSP v1.0**.

6. Submit the certificate request to the trust centre.

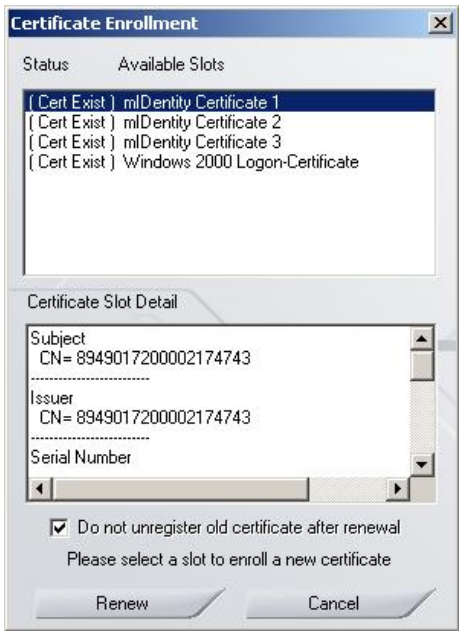

Figure 3.13: Selecting the certificate slot

Figure 3.13 shows the certificate slot selection on the KOBIL mIDentity SmartCard. Here, you can decide if the new certificate is stored on an empty certificate store or if you want to renew an existing ceritficate.

Important: Never overwrite the self-signed certificate in the first certificate slot, since it is needed to decrypt the datasafe!

7. The trust centre will send you an email with informations about how to obtain the final certificate. In some cases, you can immediately download it to the KOBIL mIDentity SmartCard. Follow the instructions from the trust centre.

8. Take a look at your new certificate in the Windows Certificate Manager as described in section 3.4.3. If the new certificate is not valied because of **missing information**, you have to manually import the trust centres root certificate as described in section 3.4.4.

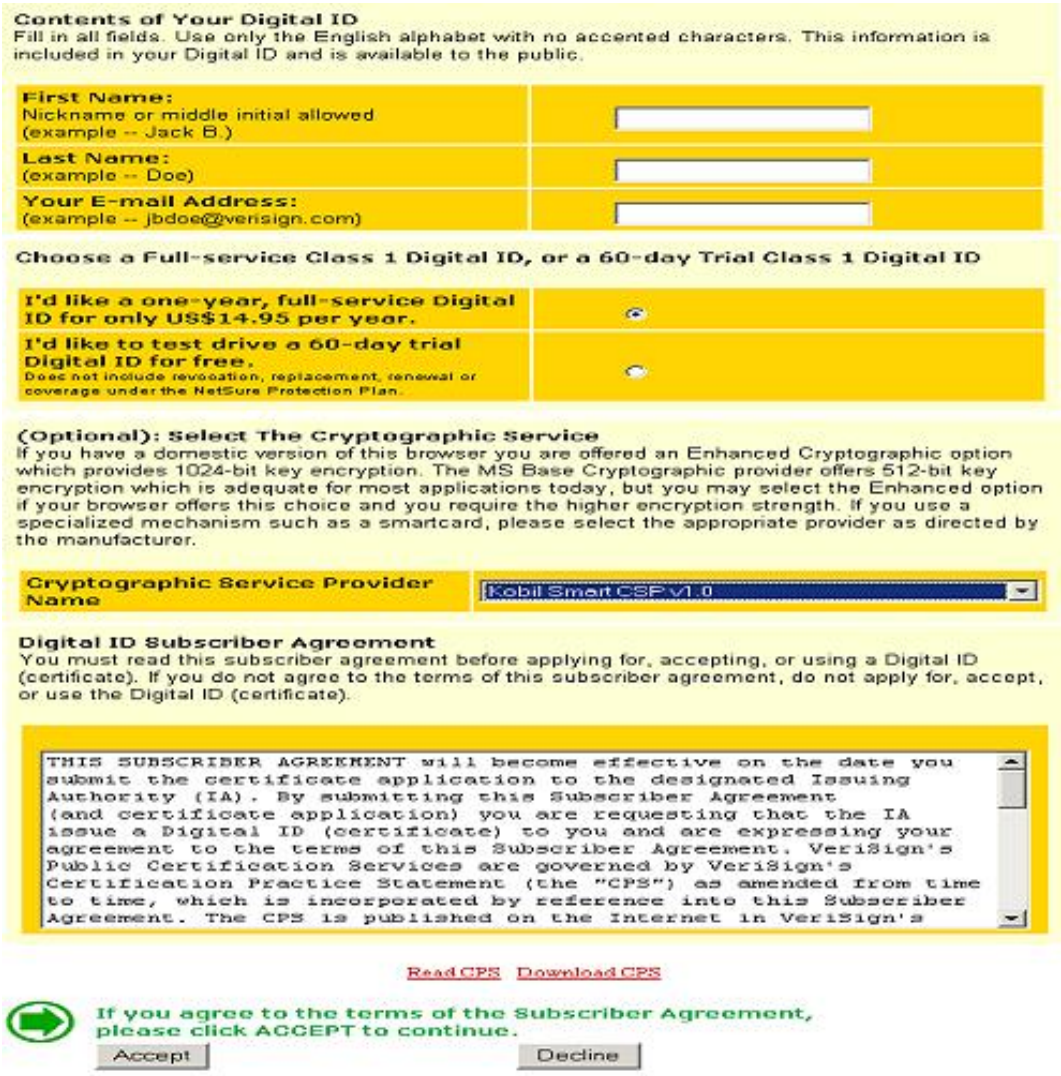
Contents of Your Digital ID
Fill in all fields. Use only the English alphabet with no accented characters. This information is included in your Digital ID and is available to the public.
First Name:
Nickname or middle initial allowed
(example -- Jack B.)
Last Name:
(example -- Doe)
Your E-mail Address:
(example -- jbdoe@verisign.com)
Choose a Full-service Class 1 Digital ID, or a 60-day Trial Class 1 Digital ID
I'd like a one-year, full-service Digital ID for only US$14.95 per year.
I'd like to test drive a 60-day trial Digital ID for free.
Does not include revocation, replacement, renewal or coverage under the NetSure Protection Plan.
(Optional): Select The Cryptographic Service
If you have a domestic version of this browser you are offered an Enhanced Cryptographic option which provides 1024-bit key encryption. The MS Base Cryptographic provider offers 512-bit key encryption which is adequate for most applications today, but you may select the Enhanced option if your browser offers this choice and you require the higher encryption strength. If you use a specialized mechanism such as a smartcard, please select the appropriate provider as directed by the manufacturer.
Cryptographic Service Provider Name
Kobil Smart CSP V1.0
Digital ID Subscriber Agreement
You must read this subscriber agreement before applying for, accepting, or using a Digital ID (certificate). If you do not agree to the terms of this subscriber agreement, do not apply for, accept, or use the Digital ID (certificate).
THIS SUBSCRIBER AGREEMENT will become effective on the date you submit the certificate application to the designated Issuing Authority (IA). By submitting this Subscriber Agreement (and certificate application) you are requesting that the IA issue a Digital ID (certificate) to you and are expressing your agreement to the terms of this Subscriber Agreement. VeriSign's Public Certification Services are governed by VeriSign's Certification Practice Statement (the "CPS") as amended from time to time, which is incorporated by reference into this Subscriber Agreement. The CPS is published on the Internet in VeriSign's
Read CPS
Download CPS
If you agree to the terms of the Subscriber Agreement, please click ACCEPT to continue.
Accept!
Decline

Figure 3.14: Certificate Request at VeriSign CA

Import existing certificates into the KOBIL mIDentity SmartCard

If you already have an existing software certificate, you can import it onto you KOBIL mIDentity SmartCard. Please refer to section 3.4.6.

3.4.3 The Windows Certificate Manager

The Windows Certificate Manager is Windows' central storage for all certificates. It can be started in three ways:

1. From **Control Panel** using

   Internet Optionen > Content > Certificates

2. From **Internet Explorer** using the pull-down menu

Extras > Internet Options > Content > Certificates

3. From **Outlook Express** usign the pull-down menu

Extras > Options > Security > Digital ID's

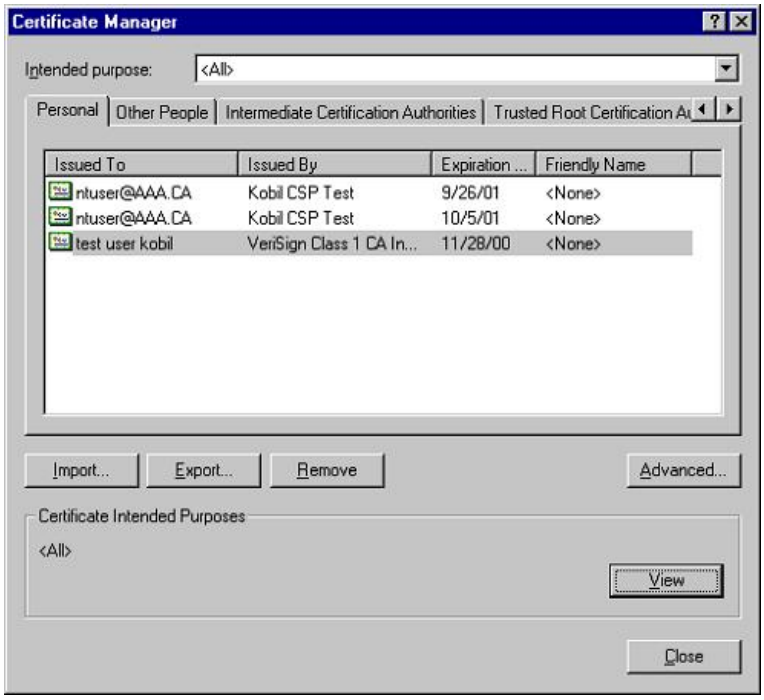

Figure 3.15: The Windows Certificate Manager

The windows certificate manager stores all your certificates, your own certificates as well as other people's certificates and trust centre certificates.

You can see the details and the trust path of a certificate from the Certificate dialog. Trust path includes the root and intermediate CA certificates that sign and approve this certificate in an hierarchical order. If any of the certificates in the path is not trusted (its signature is not valid or the root CA is unknown), that certificate and all other certificates below will be marked with a red cross, showing that those certificates can not be used.

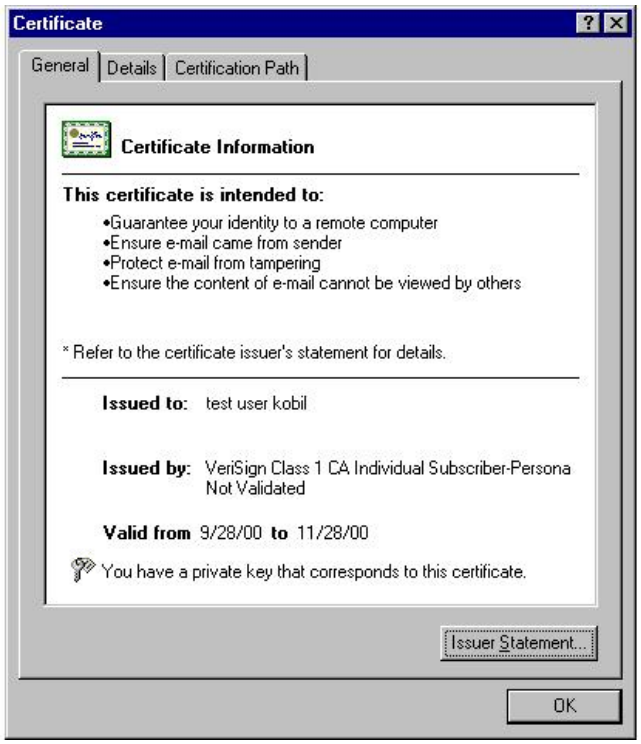
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended to:
•Guarantee your identity to a remote computer
•Ensure e-mail came from sender
•Protect e-mail from tampering
•Ensure the content of e-mail cannot be viewed by others
* Refer to the certificate issuer's statement for details.
Issued to: test user kobil
Issued by: VeriSign Class 1 CA Individual Subscriber-Persona Not Validated
Valid from 9/28/00 to 11/28/00
You have a private key that corresponds to this certificate.
Issuer Statement...
OK

Figure 3.16: Certificate details

The Windows Certificate Manager also allows to export certificates[1] and to delete them. If you delete a certificate in Windows Certificate Manager, the certificate is only **unregistered**, it is not deleted physically on the SmartCard. If will automatically be registered again as soon as you plug in your KOBIL mIDentity the next time by the Control Centre software.

If you really want to delete a certificate from the card, please refer to section 3.4.8.

3.4.4 Importing a Trust Centre (CA) Certificate

If you want to securely communicate with users of a foreign certification authority, you have to import its CA certificate (also called *root certificate*) first. If the CA certificate of a known certification authority expires, you also have to import the new CA certificate.

1. Download the root certificate from the CA's Web site.
2. The certificate will be displayed with the hint that it is **not trusted**, because it is not stored in the **Trusted Root Certification Authorities** store.
3. Click on **Install Certificate**.
4. The following dialogues can be skipped using the button *next*.
5. The last dialogue box asks you to confirm the CA certificate's fingerprint. You should obtain this fingerprint on a independent way, for example on the CA's letter paper or on its web pages.

[1] note that the SmartCard's private key can never be exported

Note that you automatically get an implicit trust relationship to all users of the new certification authority when you import its CA certificate! You should inform yourself about the certification policy of the new certification authority before importing its CA certificate.

After successful import, you find the new CA certificate in the Windows Certificate Manager either in **Intermediate Certification Authorities** or in **Trusted Root Certification Authorities** (see section 3.4.3).

3.4.5 Importing another User's Certificate

Before you can send e-mail to a user, you must get the user's digital certificate and add it to your address book. You can obtain the certificate by two ways:

- Receive a signed e-mail from the user. Signed e-mail contain the user's digital certificate.
- Obtain the user's certificate from a public directory service.
- Save the user's certificate to your certificate store.

Outlook Express

In Outlook Express, choose the menu

Edit > Find > People

Outlook 98 / 2000 / xp / 2003

In Outlook, click on **Find People** in the menu

Extras > Address Book

Figure 3.17 shows the dialogue for all Outlook versions. You can search for the recipient's name or e-mail address.

Setting-up a new directory service

If you want to use any other than the pre-installed directory services, open the menu

Extras > Accounts > Directory Service

and click on the button **Add > Directory Service...**. An assistant will be started that will guide you throught the process. You will have to enter the following informations:

- **Directory Server:** This is the address of the new directory server.
- **Authorization Required:** If this checkbox is active, you will have to enter a username and a password for user authentication. Usually, this option is not used.
- **Check Addresses with this Directory Service:** If this checkbox is active, the directory service will be used to resolve e-mail addresses from user names and to search automatically for recipient's certificates.

Once the directory service is configured, it may be necessary to enter the directory service's **Search Base**. To do that, select the newly installed directory service once more and click on **Properties**. In the drawer **Extended** you can enter the **Search Base**.

Ask your system administrator for the parameters suitable for your directory service.

You can also configure a directory service for **automatic Search for certificates** of e-mail recipients by activating in the menu

Extras > Accounts > Directory Service > Properties

tge option **Check recipient addresses with this directory service**.

Once you have successfully imported another user's certificate, you can take a look at it in the Windows certificate manager under **Other People** (see section 3.4.3).

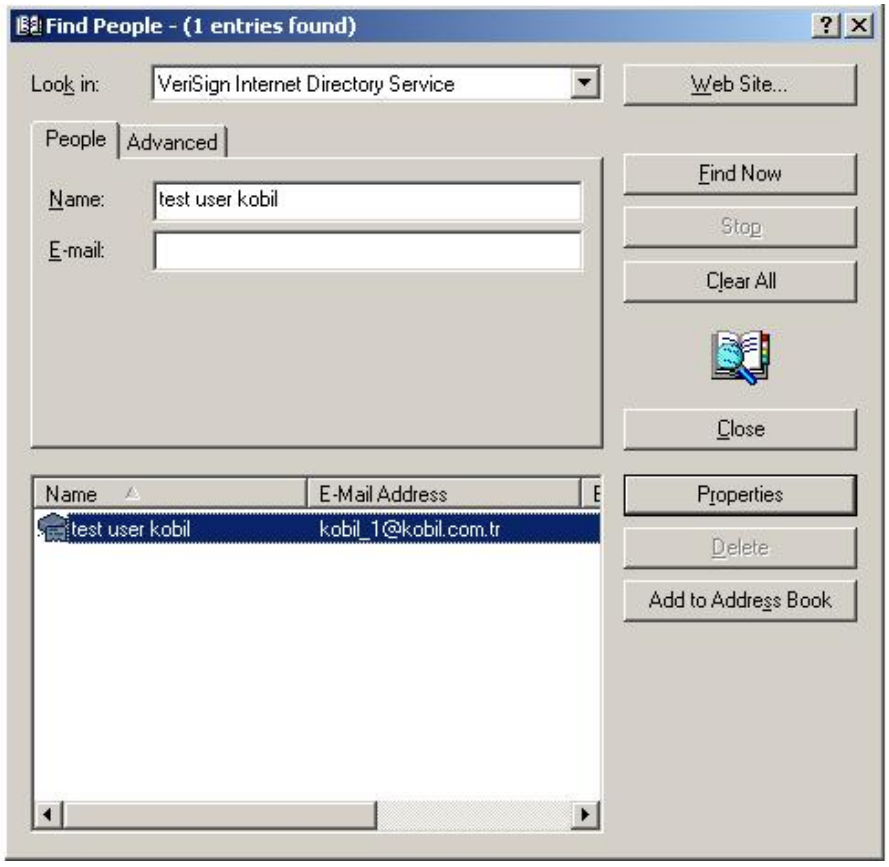

Figure 3.17: Find People Dialog

3.4.6 Import an existing certificate onto the KOBIL mIDentity SmartCard

If you already possess a software certificate [2], you can import it into KOBIL mIDentity including the private keys.

[2] these certificates are stored in PKCS#12- or PFX-files instead of a SmartCard

You can import any software certificate stored in the Windows Certificate Manager that is marked as “exportable”. Open the Control Centre Software and choose the option

Properties... > Identity

and click on the drawer **Card** the button **Import**.

If you have the software certificate only as a PKCS#12- or PFX-file, you should import it first into the Windows Certificate Manager by double-clicking it. Follow the import wizard's instructions and take care to **mark the certificate as exportable**.

For security reasons, the software certificate will be deleted from the Windows Certificate Manager after importing it into KOBIL mIDentity! Afterwards, it will only be usable with KOBIL mIDentity.

Depending on your configuration, this option may be disabled since it depends on the used SmartCard type.

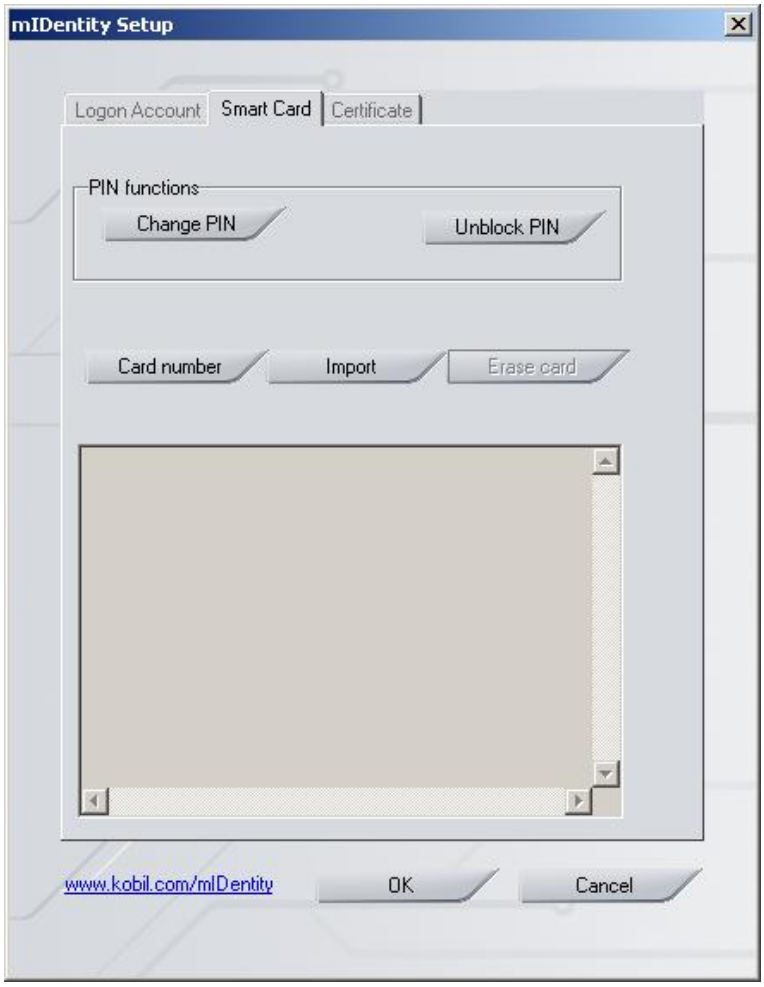

Figure 3.18: SmartCard preferences

3.4.7 Replace current SSO and Secure Data Storage certificate

If your certificate expires, you move to another department, or you change your e-mail address you will probably need to replace your current KOBIL mIDentity certificate. This can be accomplished by removing the existing certificate and creating a new one.

1. To replace a certificate select the option **Setup** from the main menu and choose the **KOBIL mIDentity Setup** menu item.

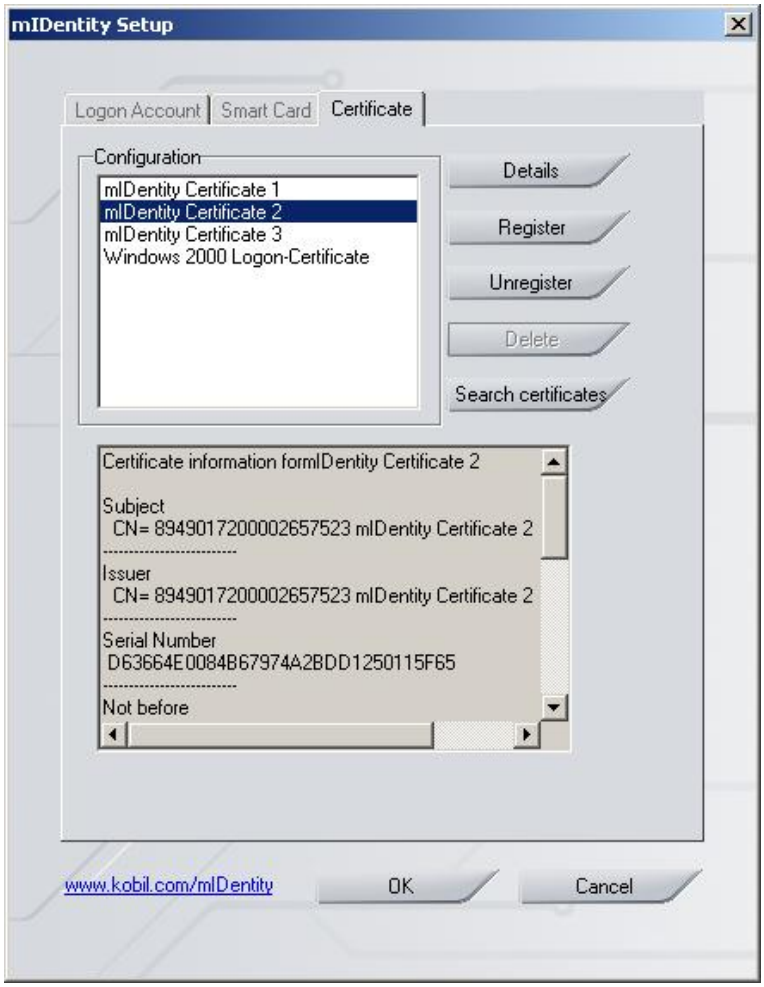

Figure 3.19: Current KOBIL mIDentity certificates

From the **KOBIL mIDentity Setup** screen select the **Certificates** option and then highlight on the given list of certificates currently residing on your KOBIL mIDentity the certificate you want to replace. Select option **Delete**.

Note: If the **Delete** option has been disabled contact your system administrator.

2. The Initialization Wizard will appear to guide you through the next steps.

mIDentity-initialisation-assistant
The existing certificate for SSO and Secure Data Storage will be removed from mIDentity. The Wizard will guide you through the steps to create a new certificate.
Current Smart Card status:
Certificate :
available
SSO and Secure Data Storage certificate assignment :
not defined
Click "Next" to continue.
Back
Next
Cancel

Figure 3.20: Current KOBIL mIDentity setup

3. On the following screen you will be given options to create a new certificate, use one of the certificates existing on your card, or import a new certificate for your data encryption.

Figure 3.21: Define new certificate

4. Once you selected the certificate you want to use, the system will encrypt the data on your KOBIL mIDentity with the new certificate and the old certificate will be permanently deleted.
   ATTENTION: Encrypted data which is not reachable at this time couldn't be reencrypt and will not be usable any longer!

Figure 3.22: Final KOBIL mIDentity status

3.4.8 Delete certificates from your KOBIL mIDentity SmartCard

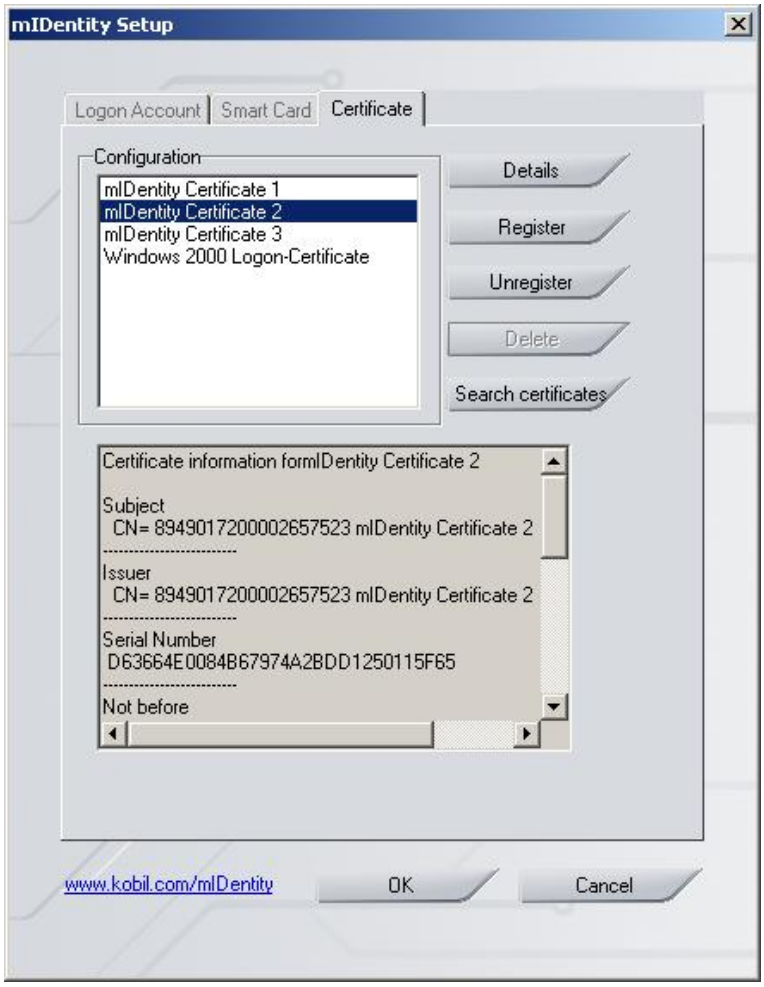

Figure 3.23: Certificate preferences

Important! Be very careful deleting a certificate, since it is needed to decrypt datasafes, emails, files and folders that are encrypted with it. If you delete a certificate, any data encrypted with it may note be accessible anymore! Especially the first certificate slot contains the self-signed KOBIL mIDentity certificate used for datasafe encryption.

Open the Control Centre Software and choose the option

Properties... > Identity

and choose the drawer **certificates**. Select the certificate to delete from the list and click on **delete**.

Depending on your configuration, this option may be disabled for security reasons. If you need to enable this option, please ask your system administrator.

3.5 KOBIL mIDentity Personalization

KOBIL mIDentity is immediately ready to use and can be personalized by the end user "in the field" by learning passwords (see section 4.1.3) and requesting certificates (see section 3.4.2). This way, KOBIL mIDentity is immediately usable where no infrastructure is available as well as for individual users.

In bigger organisations with existing infrastructure, this is not really useful. For these situations, KOBIL offers administrative tools and server software for KOBIL mIDentity. Further information about this can be found at your local KOBIL dealer or in the internet at *http://www.kobil.com/mIDentity*.

3.6 Software Updates

The KOBIL mIDentity Control Centre Software is being continuously developed and extended with new functionality. If you want to stay always up-to-date, visit *http://www.kobil.com/mIDentity* from time to time. Here, you can download software updates and you find useful tipps and hints about your KOBIL mIDentity.

Chapter 4

Your mobile Identity

KOBIL mIDentity is you electronic identity that you can carry with you anywhere you are - your personal digital ID card!

Depending on the application, several different technologies exist that can be used to authenticate yourself: static passwords, one-time-passwords (OTP), Simple Sign-On (SSO) and certificates. In this section, you learn how to use those functions and how to realize your personal mobile identity.

4.1 Passwords and Simple Sign-On (SSO)

Today, passwords are omnipresent in your daily life: Web-Mail accounts, network access, VPN connections and many applications authenticate users using static passwords. This requires the users to memorize a lot of different passwords or some users might use the same passwords for all applications which leads to severe security leaks. Some users also note their passwords on little "stick-it" papers at the monitor.

Using KOBIL mIDentity, you can forget all your passwords - because KOBIL mIDentity stores them high securely, protected trough SmartCard technology, on it's own mobile memory[1]. Instead of a lot of different passwords, you only have to remember the KOBIL mIDentity SmartCard's PIN which is the key to all your passwords!

4.1.1 What is Simple Sign-On (SSO)?

Simple Sign-On (SSO) is a techique that simplifies authentication procedures for both end users and administrators. Users need to authenticate themselves only once for all applications while administrators can work on centralized user databases.

As your passwords are stored inside the KOBIL mIDentity SmartCard, you only have to memorize its PIN code - it protects all those informations. KOBIL mIDentity automatically recognizes password entry dialog boxes and fills in your user name and password. Both HTML-forms and Windows dialog boxes (e.g. network logon) are supported. Besides static passwords, you can also use dynamic one-time-passwords (OTP) with KOBIL mIDentity. One-time-passwords require additionally the KOBIL SecOVID server as a central authentication server (AAA server) which allows real Simple Sign-On also for Administrators - much cheaper than common SSO systems!

[1] does not apply to KOBIL mIDentity Light

4.1.2 Using Simple Sign-On - Survey

The following short cuts help you to use KOBIL mIDentity in a comfortable way when you want to logon to securely to your applications:

- ALT-F11: If your KOBIL mIDentity device should learn a password dialog you can initiate the learning procedure (if the logon window is activated by a mouse-click) by pressing ALT-F11 . For details we refer to section 4.1.3.
- ALT-F10: Usually KOBIL mIDentity recognizes learned password dialogs and indicates this, and you only have to confirm your intention to be logged on by clicking the "Logon" button. Nevertheless, in some cases (e.g. when working with terminal consoles, see section 4.1.4) KOBIL mIDentity does not know which of the learned password dialogs is to use. By pressing ALT-F10 (if the logon window is activated by a mouse-click) you get the list of the learned password dialogs, and you can select the desired password entry.
- ALT-F12: In some cases KOBIL mIDentity does not recognize learned password dialogs. Besides the possibility to press ALT-F10 (see above) you invite KOBIL mIDentity by pressing ALT-F12 to check again all open windows whether they contain a password dialog KOBIL mIDentity had already learned.

Advanced features of Simple Sign-On

The Simple Sign-On solution is very tight related to the hardware and software environment on which it operates. To avoid possible configuration problems and also to give you additional setup options we offer advanced features.

To reach the advanced features, select the option **Setup** from the main menu and then choose the **KOBIL mIdentity Setup** menu item. From the **KOBIL mIdentity Setup** screen select the **Advanced Features** option on the **Logon Accounts** screen.

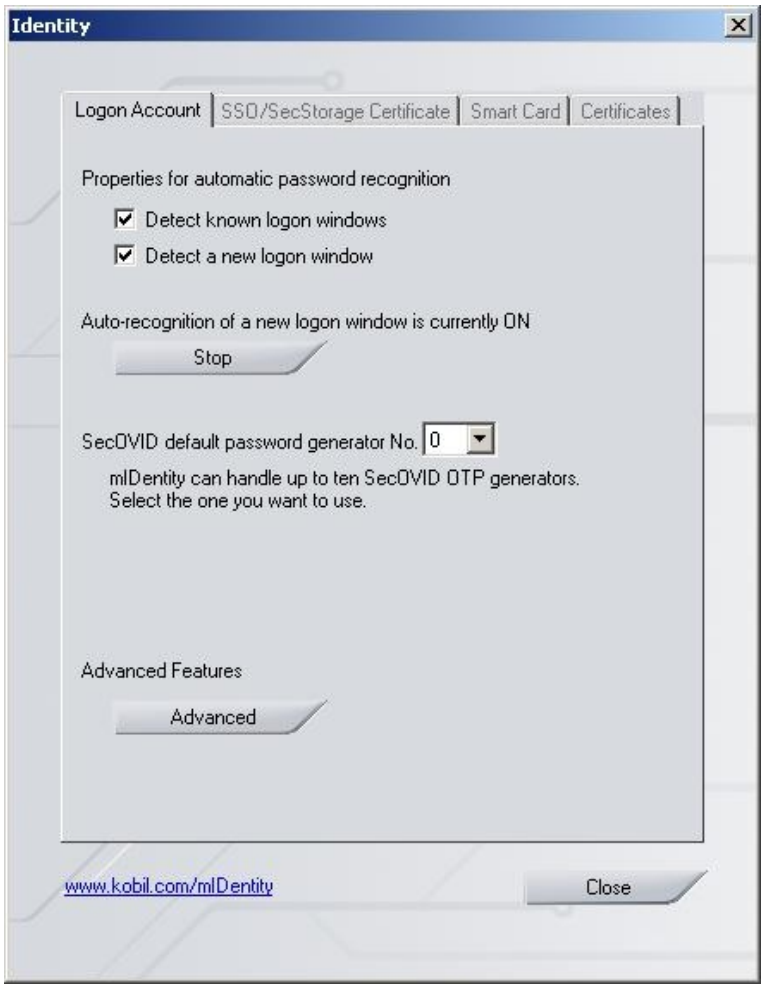

Figure 4.1: Simple Sign-On Settings

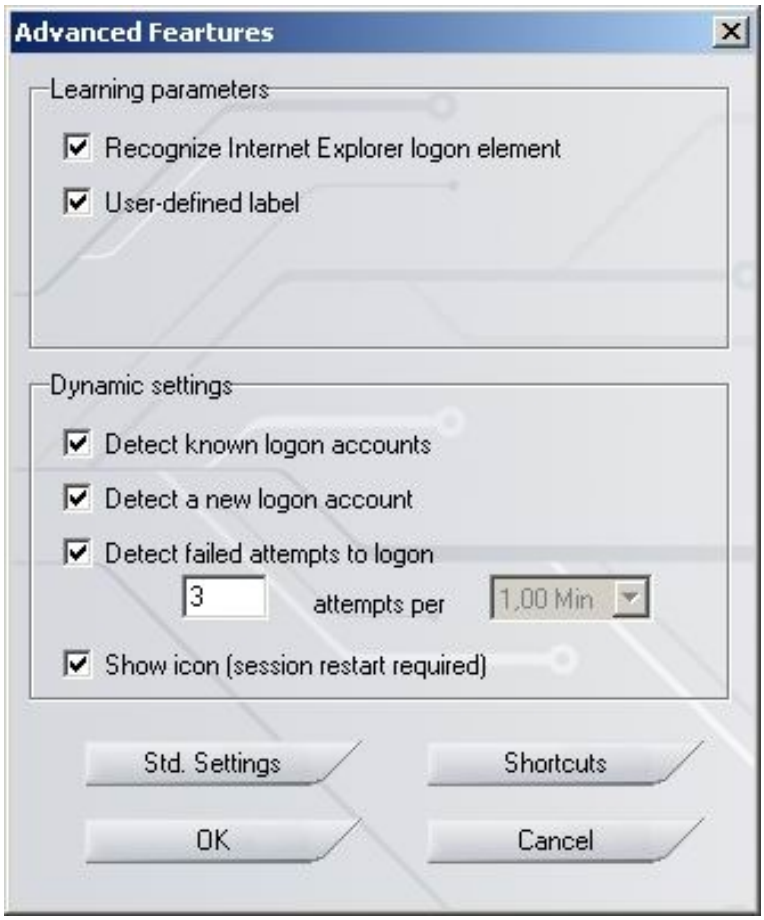

Figure 4.2: Simple Sign-On advanced features

- **Learning parameters**

  1. Recognize Internet Explorer logon element
     The **Recognize Internet Explorer logon element** option will save you one step in the application logon dialog learning process by automatically recognizing the login element.
  2. User-defined label
     - The **User-defined label** option gives you an option to name your logon account rather than having the system do it for you.

- **Dynamic settings**

  1. Detect known logon dialogs
     The SSO will logon automatically to a known account.
  2. Detect a new logon dialog
     The SSO will start a learning process as soon as an unknown window with a password field appears on screen.
  3. Detect failed attempts to logon
     The Simple Sign-On feature can be configured to automatically detect a new application window and proceed with the logon dialog. To avoid an infinite loop in case of a failure, the max number of allowed failed logon attempts must be specified.

4. Show icon
   The Advanced Features can be invoked as a separate mini-application directly from the tray-bar. It offers additional functionality which can be reached via a menu triggered by clicking the right mouse button on the Advanced Features icon.

Figure 4.3: additional icon for SSO

- **Buttons**

  1. Cancel:
     Settings will be closed without saving the changes.
  2. OK:
     Save settings and finish.
  3. Hotkeys...:
     Alter the hotkeys.

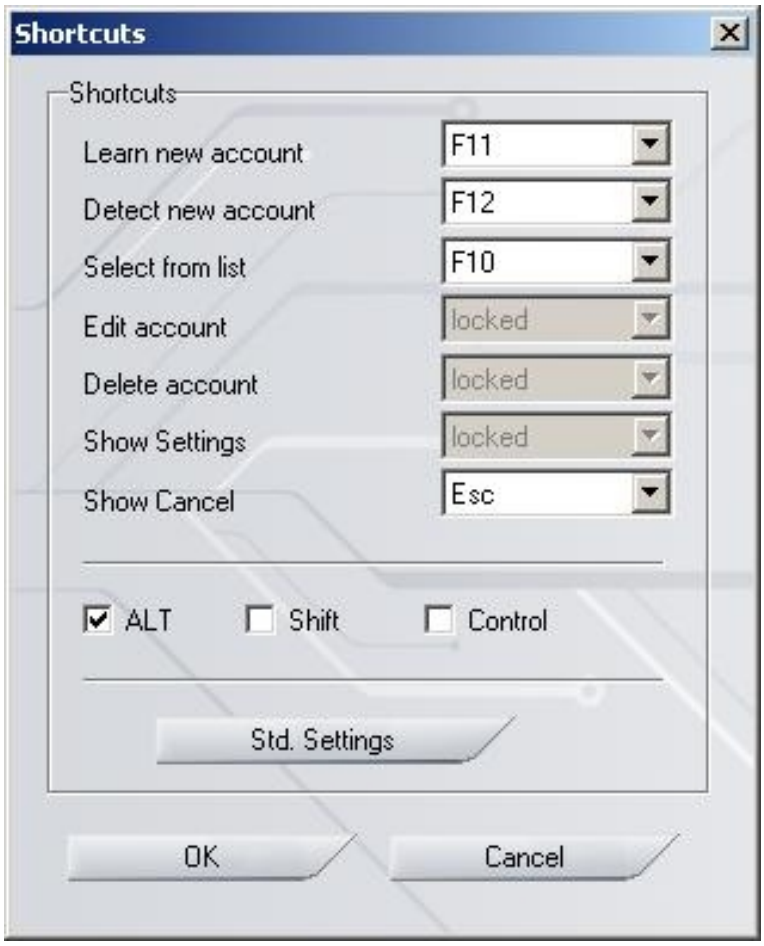

Figure 4.4: Alter hotkeys

4. Standard:
   Reset settings.

4.1.3 Learning Passwords

If you want to personalize passwords centrally for many users, please refer to section 3.5. But KOBIL mIDentity can also learn password information very easily by end users. This is done by a wizard that guides you step-by-step through the learning process. After completing the process, your passwords are stored securely inside KOBIL mIDentity.

1. Open the logon dialog box for which you want KOBIL mIDentity to learn the password. This can be any Web-based application (HTML) or a windows dialog box (e.g. network logon).

Figure 4.5: Network Logon dialog

2. Press **ALT-F11**. The KOBIL mIDentity password assistant is being started

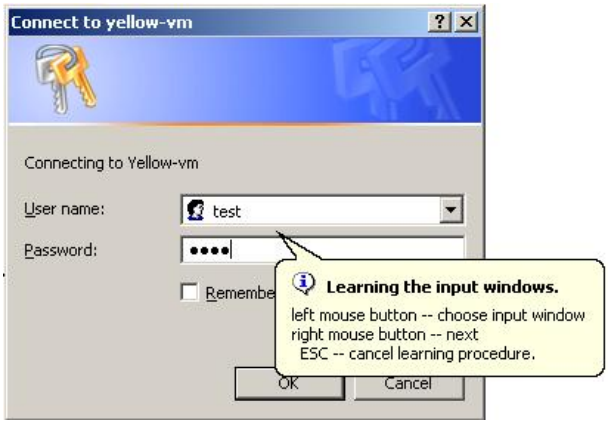

Figure 4.6: The KOBIL mIDentity Password Assistant

3. Click with the **left mouse button** onto a text area that you want to be filled out by KOBIL mIDentity, for example the user name (in this example the the text area *connect as* from the Windows network logon dialog box). Then enter the value that shall be filled in by KOBIL mIDentity.

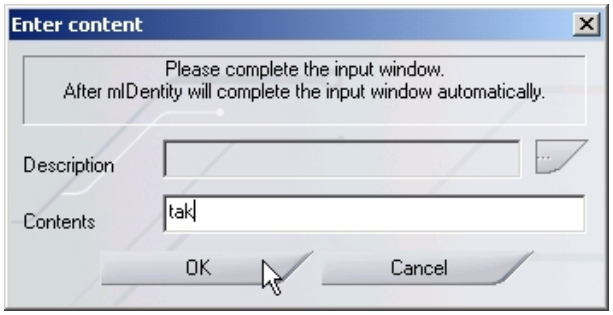

Figure 4.7: Learning the user name

You can fill out more text areas by repeating that step as often as required.

4. KOBIL mIDentity recognizes automatically password fields and opens the password dialog. You can select either a static password (enter twice) or a one-time-password (OTP) generated by the KOBIL SecOVID system which requires a KOBIL SecOVID generator on your KOBIL mIDentity SmartCard.

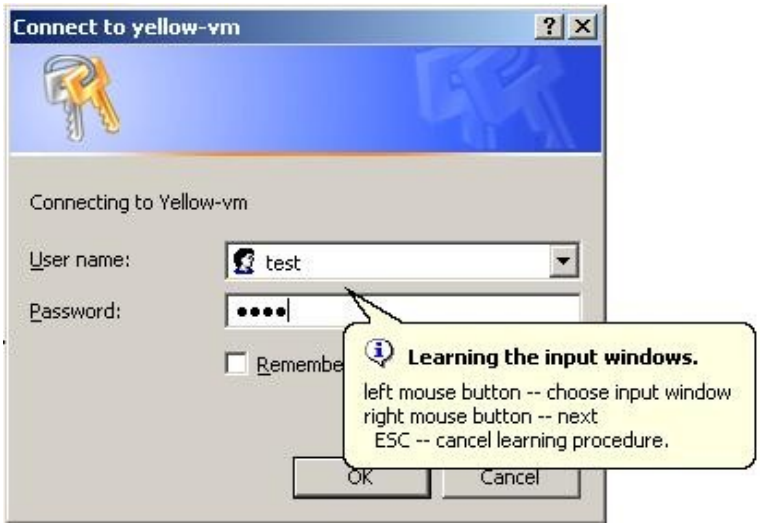

Figure 4.8: Learning the password

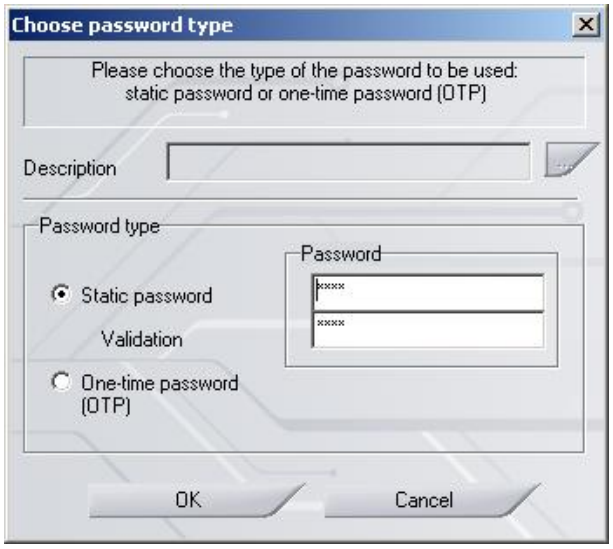

Figure 4.9: Learning the password

Note that one-time-passwords (OTP) require additionally the KOBIL SecOVID Server. Please refer to your local KOBIL dealer or direclty to *http://www.kobil.com/SecOVID* if you have questions about KOBIL SecOVID.

5. Right-click in order to finish learning the password dialog. Now you can finally select the **OK** button with a left mouse click which finishes the learning process.

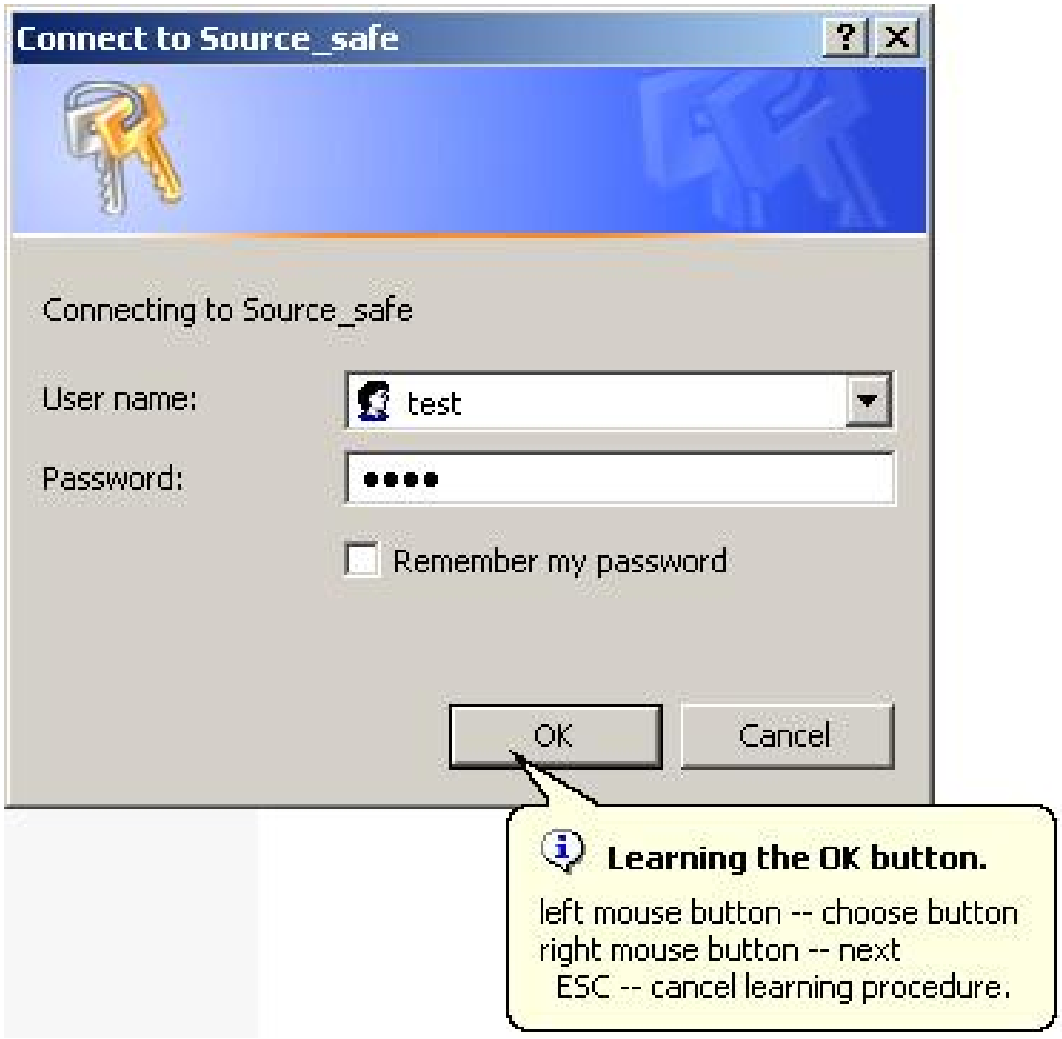

Figure 4.10: Learning the OK Button

If the same password dialog appears the next time, KOBIL mIDentity automatically recognizes it and asks if it should fill-in the user name and password. There are differences between Windows-applications and and WEB-applications.

Figure 4.11: automatic Windows-application logon with KOBIL mIDentity

In case of a WEB-application you can choose between **Fill in** and **Login** furthermore. Choose **Fill in**, to fill in the learned elements but do not send the login information. So you can enter additional elements by yourself, because they change every time you visit the site for example.

Figure 4.12: automatic WEB-application logon with KOBIL mIDentity

NOTE: While logon to java applications there is a technical need to execute mouse movements and mouse clicks. For that reason you should not do any input while KOBIL mIDentity automatic login to a application.

4.1.4 Working with Console Applications

As not all applications are based on Windows dialog boxes or HTML, KOBIL mIDentity can also work with console windows (DOS-Box, PuTTY). See a FTP console as an example:

Please open your command prompt and press **Alt-F11**. Enter user name and password in the input dialog. You can use static passwords or one-time-passwords (OTP) with the additional KOBIL SecOVID system.

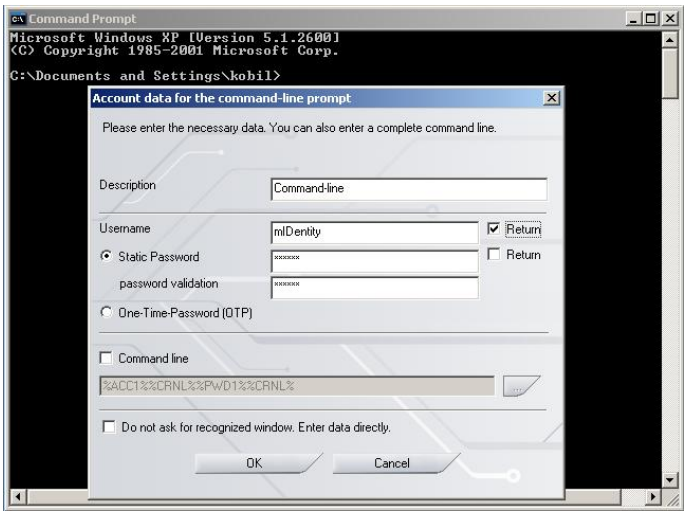

Figure 4.13: Manual entry of passwords for console applications

You can also enter complete command lines if you have choosen the option **Command line**. Therefor you can use following aliases:

1. %ACC1% = User name
2. %PWD1% = Password
3. %CRNL% = Carriage Return / New Line (Windows)
4. %NL% = New Line (Unix e.g.: PuTTY)

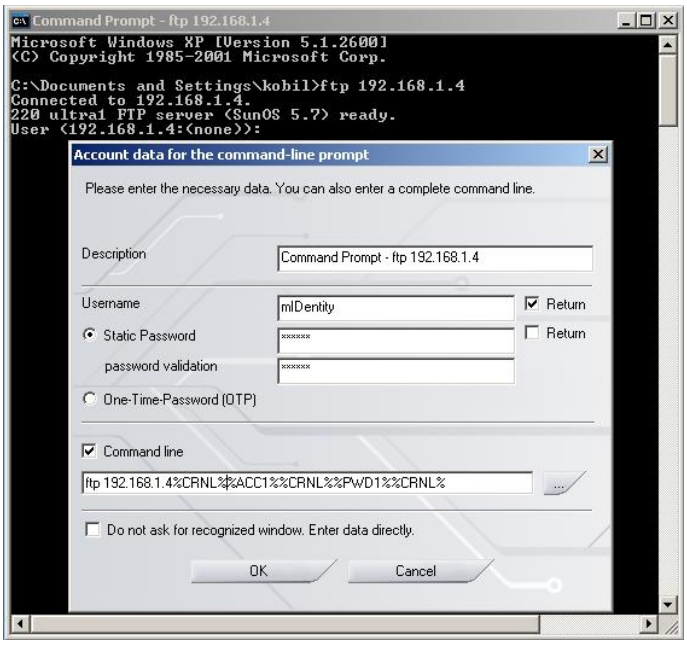

Figure 4.14: Manual entry of command lines for console applications

To paste a password or a command line from KOBIL mIDentity into a console application, start your command prompt and press **Alt-F10**. Choose your account and press **OK**. Your account data will be filled in automatically as if you would have entered it using the computer's keyboard.

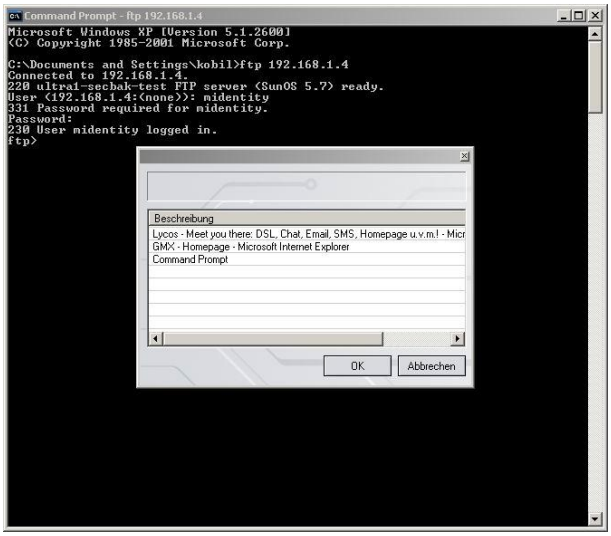
Command Prompt - ftp 192.168.1.4
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\kobil>ftp 192.168.1.4
Connected to 192.168.1.4.
220 ultra1-sechak-test FTP server (SunOS 5.7) ready.
User (192.168.1.4:(none)): midentity
331 Password required for midentity.
Password:
230 User midentity logged in.
ftp>
Beschreibung
Lycos - Meet you there: DSL, Chat, Email, SMS, Homepage u.v.m.! - Micr
GMX - Homepage - Microsoft Internet Explorer
Command Prompt
OK
Abbrechen

Figure 4.15: Manual Password Transfer

Please note that this function can have problems with different character encodings. This is why you should use only

passwords consisting of standard ASCII characters. One-time-passwords (OTP) consist of 8 digits and can be used without any problem.

4.1.5 Managing Logon Accounts

To manage your logon accounts on mIDentity click on the push button **My Logon Accounts ...** on Control Center or in the Traybar-Menü.

You will be requested to enter the PIN of the smartcard from your mIDentity to authenticate yourself for access to your personal data. Only you can read and change your logon information.

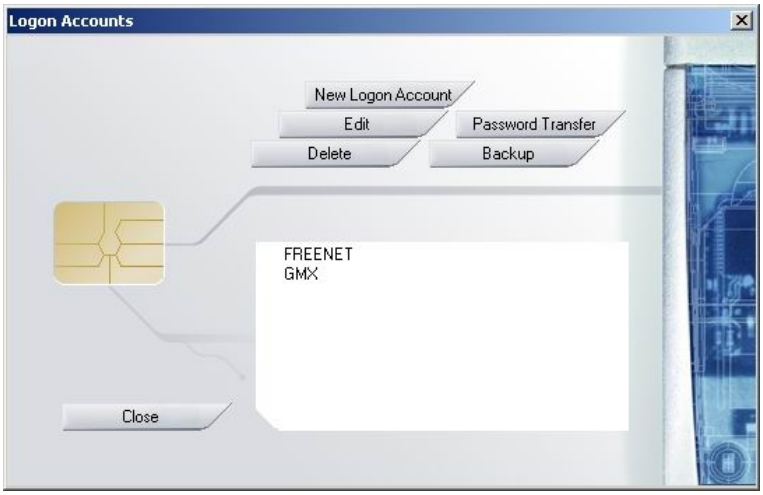

Figure 4.16: Edit Password Informations

Editing Logon Data

When you need to change your logon data (e.g. your password has expired), you have two options to do that. Select the account you want to change and click on the push button **Edit** or simply double-click on the account you want to edit. You can change individual attributes in the dialog that follows.

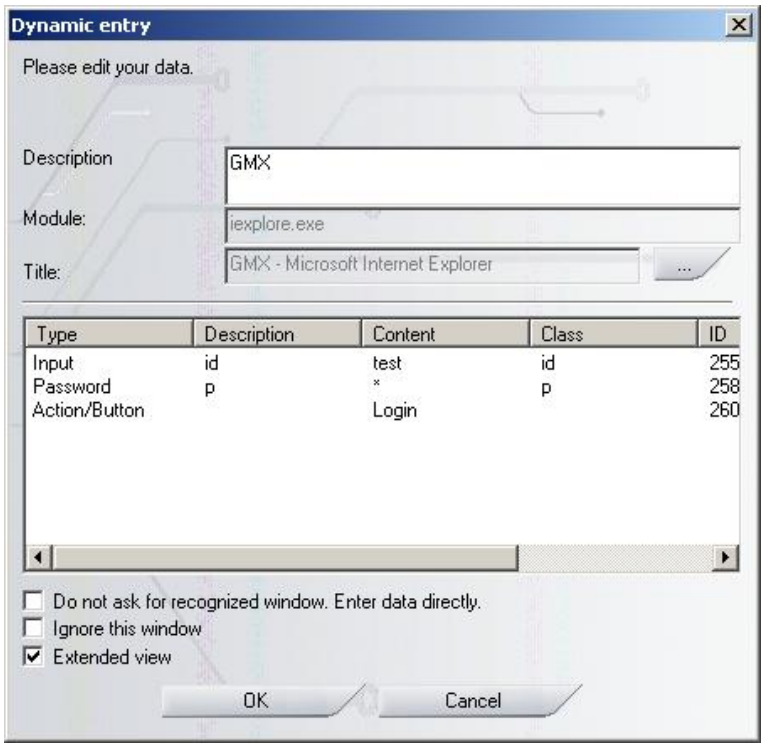

Figure 4.17: Editing Dynamic Accounts

The following logon accounts attributes can be changed:

- Account Name - Specify the account name.
- Entry - Double-click on this attribute to change the field value (usually user name)
- Password - Double-click on this attribute to change the password field value (optionally also a generator number of an OTP account)

Additionally, you can define the following properties of an account:

- You can have your learnt account fields filled out automatically when the logon window is detected, or you can have the system ask you each time for a confirmation.
- You can set an option to ignore the detected logon window.
- you can specify if you wanted en extended view of the account properties. This view can help in error analysis, in case a logon window is not properly handled.

Advanced Features

Click on the push button **...** on the right side of the title to get to the advanced features. In this dialog you can change the properties, which usually remain unchanged. The advanced features give you an option to change some specific behaviour,

or to use specific technology of the SSO-solution in order to go around some known problems.

Please note: Changes done to those advanced properties can dramatically influence the account functionality. Please do not make any changes if you are not completely sure of an impact it may have on your system.

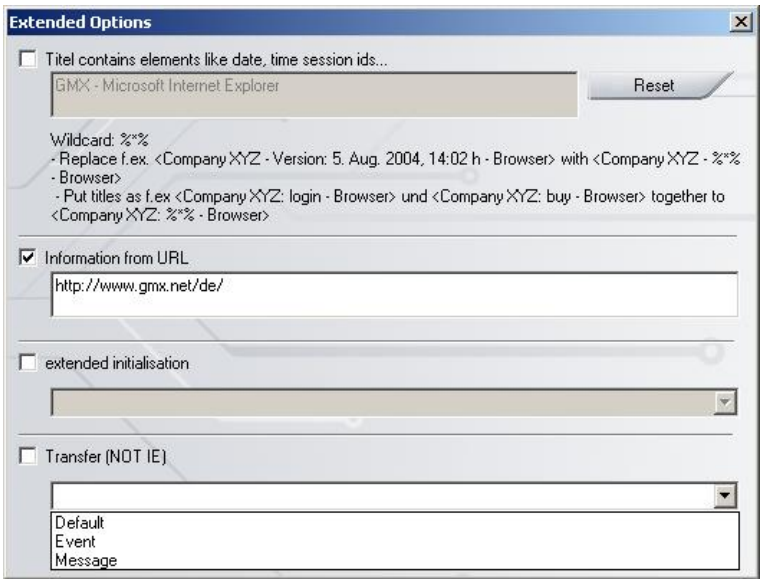

Figure 4.18: Advanced Configuration

- Title contains data, ...
  During the learning process of an application window some specific properties of that window are saved and used later to detect the site. One of that features is the window title. There are windows which contain dynamic parts, which change each time the window is opened. It is therefore hard to use title as an identifying feature. With help of wildcards those dynamic parts can be ignored. If a window title contains current time, this part of the title must be taken out of the defined identifying feature. Example:
  The window title is: **Your Application - 10:10**
  You must build a mask to define the time-part as dynamic: **Your Application - %*% -**
  This way the time-part of the title will not be considered in the window detection algorithm.

- Extract Information from URL
  This parameter is usually activated for browser applications, because this window is generally detected by the URL, and not the title. To force detecting a browser application by its title deactivate this parameter.

- Advanced Initialization
  This feature is meant to be used by administrator. In standardised environments it is possible to use predefined logon templates. Those templates are then filled out with personal data by the end. For more details regarding this solution please contact your KOBIL Partner.

- Transfer
  This feature does not apply for browser applications. For all other applications you can define a method of interspersing personal data into the appropriate application field. As a standard this happens via Windows messages, but because some applications have problems with this methodology, we introduced the possibility of using event-based technology. The event-based technology simulates manual key entry, which helps to solve the problem, but is much slower than the message solution.

4.1.6 Backup Logon Accounts (Simple Sign-On

Simple Sign-On simplifies access to services and applications on your computer. You will only need to know the PIN of your SmartCard; application access will be handled for you in the background. It is therefore very important to double-protect your logon data by taking regular backups. We recommend you take a backup of your logon dialogs each time a new application access dialog has been added to your list or when the logon data has changed.

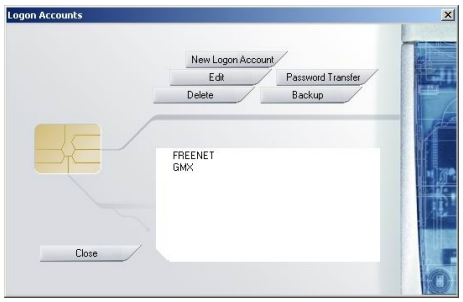

Figure 4.19: edit and view login data

To take a backup of your access data choose the option **Logon Accounts** from the main menu. Next, select the **Backup**option from the **User Accounts** screen and continue with the **Backup** option on the following screen. You can choose a place where you want the backup to be stored.

Figure 4.20: Backup your login data

Figure 4.21: Backup your login data

The KOBIL mIDentity software gives you an option to create an emergency certificate. This certificate will be crucial in case you lost the encrypted data or the KOBIL mIDentity device. In such case you will be able to restore the backup and decrypt the data with your emergency certificate.

Figure 4.22: Backup your login data

Your successful backup will be confirmed to you by the system.

mIDentity-backup-assistant
Step 4 (of 4) :
The backup of your logon accounts has been saved in C:\Documents and Settings\kobil\mIDentity\kobil-BackupData.p7 file.
To restore your data in case of emergency you will require the emergency certificate. The certificate was saved in C:\Documents and Settings\kobil\mIDentity\kobil-RestoreCredential.p12 file.
Abort

Figure 4.23: Backup your login data

4.1.7 Restore Logon Accounts

To restore applications access accounts from a backup select the option **Logon Accounts** from the main menu, then the **Backup**option on the **User Accounts** screen and the **Restore** option on the following screen. You will be presented with a screen allowing you to select the backup file.
In a situation where no certificate can be found on your KOBIL mIDentity, you will be asked to provide your emergency certificate and your emergency password to restore the backup.

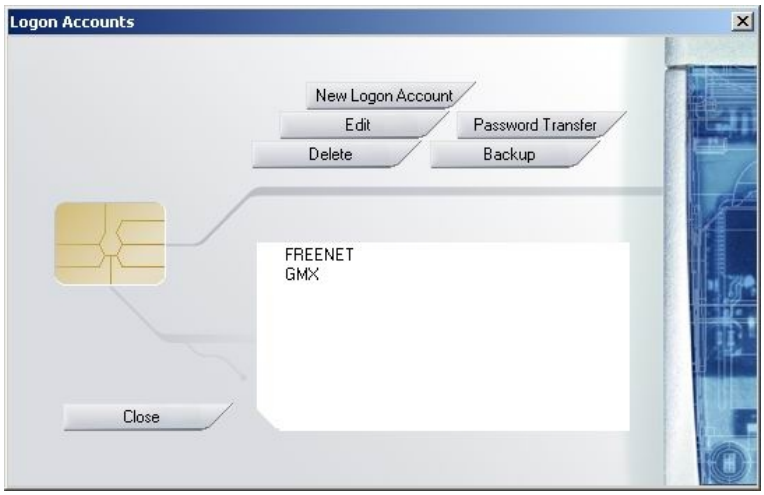

Figure 4.24: edit and view login data

Figure 4.25: restore login data

Figure 4.26: restore login data

Figure 4.27: restore login data

4.1.8 KOBIL mIDentity SSO Emergency Assistant

In case you need to access a backup but do not have KOBIL mIDentity to access the Control Centre, we offer the SSO Emergency Assistant. This service allows you to access a backup and displays logon data in plain text. You will then use the data to individually sign into your applications. The SSO Emergency Assistant can be started from the Traybar only if there is no KOBIL mIDentity device plugged into the PC.

Figure 4.28: view login data

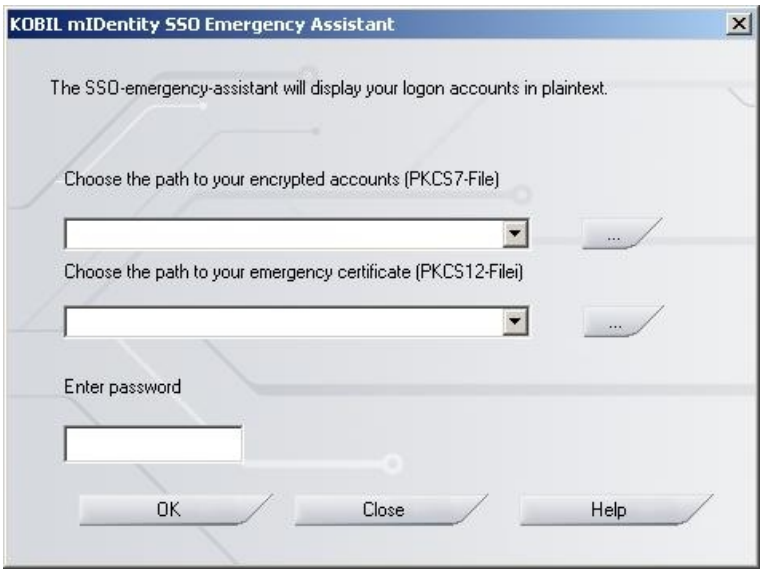

Figure 4.29: view login data

To retrieve the data, the SSO Emergency Assistant will ask you to select the backup file and your emergency password. For security reasons your logon accounts will only be displayed for 5 minutes.

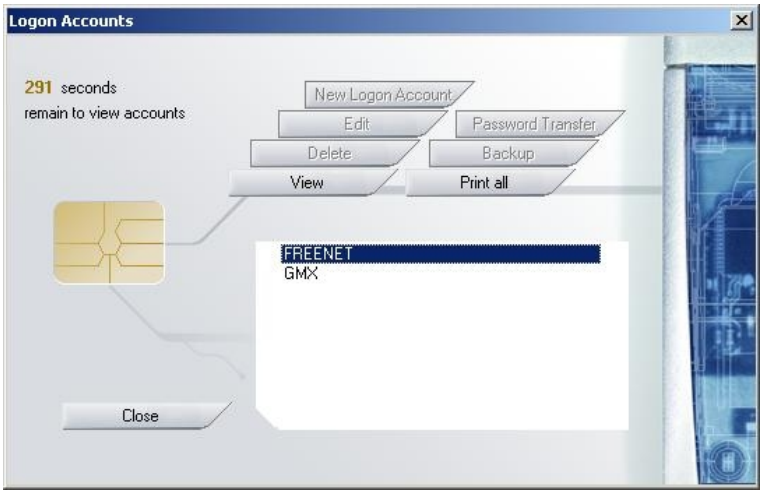

Figure 4.30: view login data

The SSO Emergency Assistant gives you also an option to print the list of your accounts.

Important Note: Be cautious while using the SSO Emergency Assistant. By having your user ids and passwords displayed on the screen and printed you are giving away very valuable information. Make sure nobody has access to your secret data.

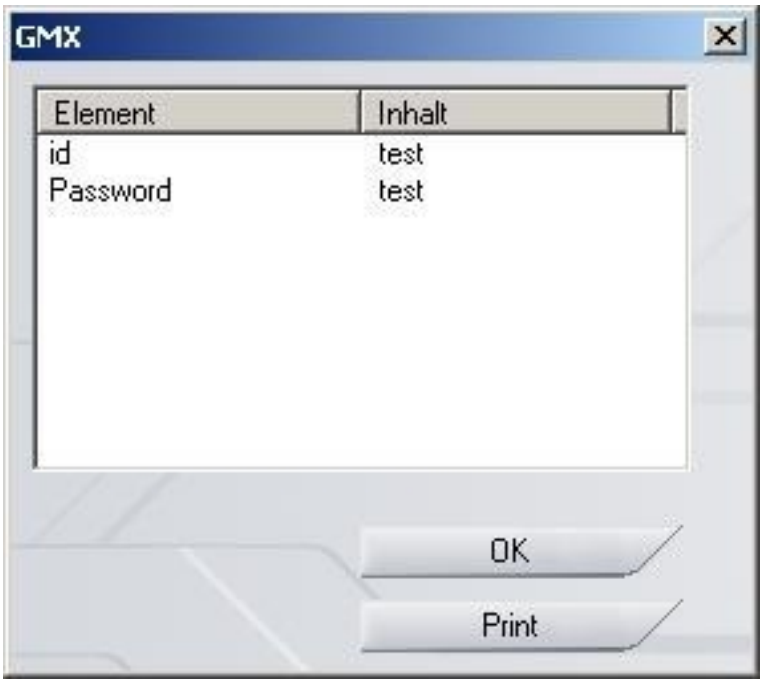

Figure 4.31: view several accounts

4.2 Windows SmartCard Logon

Windows 2000 and XP make it possible to deploy strong authentication using SmartCards by leveraging operating system features such as Kerberos, Active Directory, and the variety of administrative tools used to manage a public key infrastructure. Instead of logging on with username and password, you simply plug your KOBIL mIDentity in and enter your KOBIL mIDentity SmartCard's PIN.

If you want to log on to your computer using KOBIL mIDentity, a SmartCard logon certificate must be stored on your KOBIL mIDentity SmartCard. The computer needs to be member of a Windows 2000 or 2003 domain with Active Directory to allow SmartCard logon. The SmartCard logon certificate will be issued from the Windows certificate services with are part of Windows 2000 and 2003 servers.

More information about setting up Windows SmartCard logon can be found in the KOBIL mIDentity White Paper that you can get from your local KOBIL dealer or directly in the internet at *http://www.kobil.com/mIDentity*.

Figure 4.32: Windows SmartCard Logon: PIN entry

Chapter 5

Your mobile Secure Data Storage

KOBIL mIDentity's Secure Data Storage gives you the possibility to securely store your sensitive data and carry it with you anywhere you go[1]. Business documents, private information - everything is encrypted by KOBIL mIDentity using highly secure SmartCard technology.

5.1 Strong Encryption for sensitive Data

KOBIL mIDentity offers a lot of advantages compared with common encryption products, since it is mobile, independent, efficient and highly secure.

You have the following possibilities to protect your sensitive data using KOBIL mIDentity:

- **Mobile Secure Data Storage on KOBIL mIDentity[2]:** carry your sensitive data always with you in your pocket.
- **Secure Data Storages on your Hard Disk:** local Secure Data Storages on your notebook or your home PC or business PC offer you enough space for sensitive data and are protected efficiently by the KOBIL mIDentity SmartCard during your absence.
- **Secure Data Storages on network drives:** Secure Data Storages on network drives offer an additional advantage to Secure Data Storages on local hard disks. With Secure Data Storages on network drives it is possible to reach your sensitive data from different workstations.
- **File Encryption:** Encrypt even single files and directories with the same highly secure SmartCard technology. You can exchange encrypted files with your friends and colleagues. Further information about this can be found in section 5.3.
- **Email Encryption:** see section 6.1.

5.2 Secure Data Storages with KOBIL mIDentity

KOBIL mIDentity allows secure storage for sensitive data inside so-called "Secure Data Storages" (also called *Container*). A Secure Data Storage is a virtual hard disk with an own drive letter that is stored physically in one huge encrypted file

[1] does not apply to KOBIL mIDentity Light
[2] does not apply to KOBIL mIDentity Light

inside your regular file system.

The Secure Data Storage is encrypted using the KOBIL mIDentity SmartCard, so the Secure Data Storages content is always strongly encrypted. Without the KOBIL mIDentity SmartCard and its PIN, nobody can access the Secure Data Storage. All KOBIL mIDentity models support encrypted Secure Data Storages on your local hard disk. For real mobility you can have a Secure Data Storage on the KOBIL mIDentity[3] itself. With them, you can carry your senstive data around anywhere you go!

KOBIL mIDentity Secure Data Storages work different than Windows 2000/XP Encrypting File System (EFS). Unlike EFS, the decryption keys are not bound to the user's Windows account, but to the KOBIL mIDentity SmartCard. By using SmartCard technology, strong two-factor authentication is achieved (possession of SmartCard AND knowledge of PIN) instead of only knowledge of the Windows user password. Data recovery can be done seperately from the Administrator role (see section 5.4).

5.2.1 Creating a Secure Data Storage on your local hard disk

Important: please read carefully section 5.4 before starting to work with Secure Data Storage in order to keep your data accessible also in emergency situations!

All KOBIL mIDentity versions can work with up to four Secure Data Storages on your local hard disk or on mounted network drives. Each Secure Data Storage can be up to 4 GB in size (if your hard disk is NTFS formatted there is no upper limit)! Additional you can also have a mobile Secure Data Storage onboard[4] to carry your sensitive data anywhere you go - see section 5.2.3.

In order to create a Secure Data Storage on your local hard disk, please proceed as follows:

1. Click in the Control Centre main window on

   Secure Data Storage > create

   The Secure Data Storage creation dialog window will appear.

[3] does not apply to KOBIL mIDentity Light
[4] does not apply to KOBIL mIDentity Light

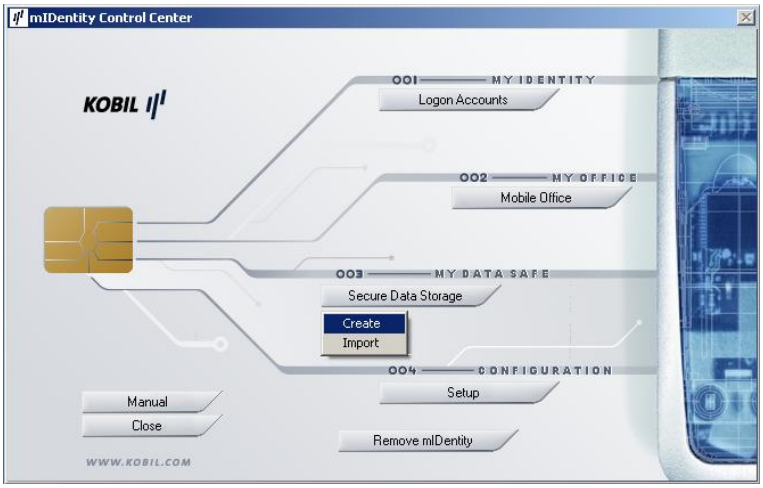

Figure 5.1: Creating a new Secure Data Storage

2. Activate the Checkbox **Secure Data Storage on Hard Disk**. You can select the path where the Secure Data Storage files will be stored.

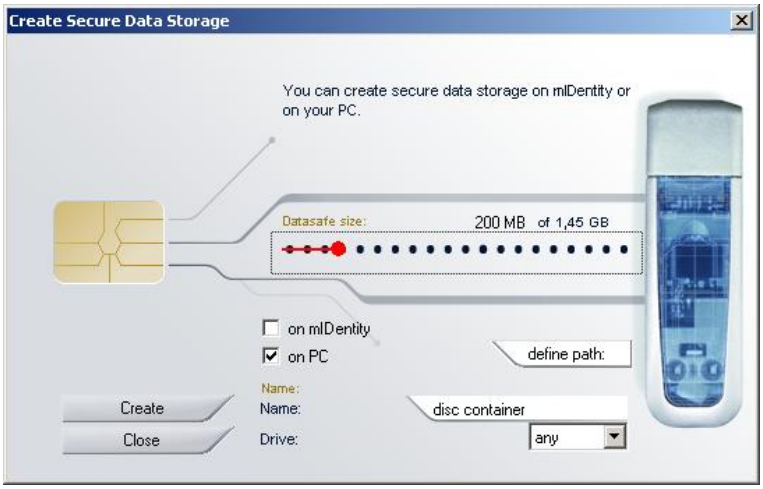

Figure 5.2: Creating a new Secure Data Storage on the local hard disk

3. Using the slide bar, you can determine the size of the new Secure Data Storage. **Important: We strongly recommend NOT to use the whole free space on your hard disk for a Secure Data Storage, since this may result in problems with the Windows operating system. You should always keep 50-100 MB free space on your hard disk.**

4. Under **Storage Name** you can define a label that will be used to display the Secure Data Storage in the Windows Explorer.

5. You can select a particular **Drive Letter** or ANY, if the Secure Data Storage shall always be mounted to the next available drive letter. A specific drive letter may be useful if you work with scripts.

6. Click **Create** in order to start Secure Data Storage creation. This process may take some time. In order to encrypt your Secure Data Storage, a random encryption key wil be generated by the smart card while creation.

7. At the end you have to enter the KOBIL mIDentity SmartCard's PIN to mount and format the Secure Data Storage which completes the process. At the end, the new Secure Data Storage icon appears on the desktop for quick access.

Figure 5.3: Desktop Shortcut for new Secure Data Storage

5.2.2 Creating a Secure Data Storage on your network drive

Important: please read carefully section 5.4 before starting to work with Secure Data Storages in order to keep your data accessible also in emergency situations!

All KOBIL mIDentity versions can work with up to four Secure Data Storages on your local hard disk or on mounted network drives. Each Secure Data Storage can be up to 4 GB in size (if your hard disk is NTFS formatted there is no upper limit)! Additional you can also have a mobile Secure Data Storage onboard[5], to carry your sensitive data anywhere you go - see section 5.2.3.

In order to create a Secure Data Storage on your network drive, please proceed as already explained for Secure Data Storages on your local hard disk. If a network drive is mounted on your system you can choose it for destination when creating a new Secure Data Storage.

If you work with Secure Data Storages on network drives it could be that you change to a workstation on wich your network Secure Data Storage is not known. To make the Secure Data Storage appear on this workstation, please proceed as follows:

1. Click in the Control Centre main window on

   Secure Data Storage > import

   The import Secure Data Storage dialog window will appear.

[5] does not apply to KOBIL mIDentity Light

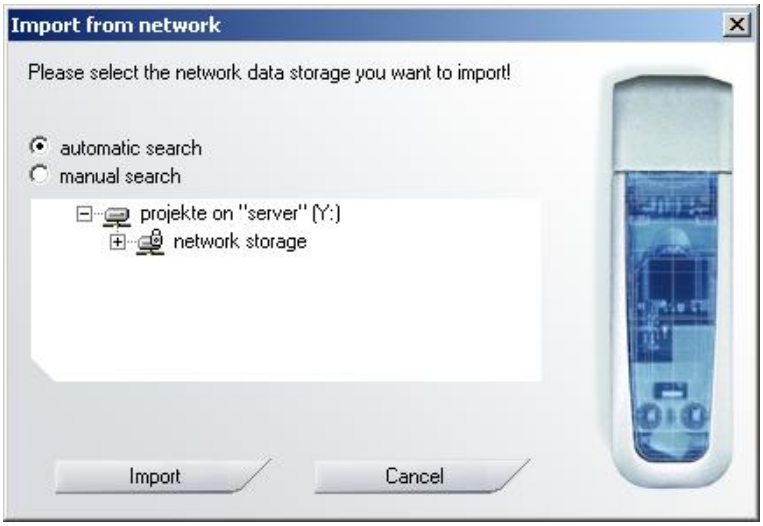

Figure 5.4: Importing a network Secure Data Storage

2. Choose the network Secure Data Storage you want to import and click **Import**. Afterwards the Secure Data Storage administration include a further point to mount or unmount this network Secure Data Storage.

Please note: as local Secure Data Storages are stored on your computer's hard disk, they cannot be carried around with KOBIL mIDentity. For those mobile Secure Data Storages, please refer to the next section.

5.2.3 Creating a mobile Secure Data Storage on KOBIL mIDentity

Important: please read carefully section 5.4 before starting to work with Secure Data Storages in order to keep your data accessible also in emergency situations!

In addition to local Secure Data Storages stored on your local hard disk, KOBIL mIDentity can also work with mobile Secure Data Storages that can be carried around directly on KOBIL mIDentity[6]. Even if your notebook is stolen, sensitive data are not only protected (by hard disk encryption) but they are also still available since you carry your backup in your pocket!

Mobile Secure Data Storages are more restriced in size, depending on the KOBIL mIDentity model. Apart from that, creating a mobile Secure Data Storage is quite similar to creating a local Secure Data Storage (see previous section):

1. Click in the Control Centre main window on

   Secure Data Storage > create

   The Secure Data Storage creation dialog window will appear.

[6] does not apply to KOBIL mIDentity Light

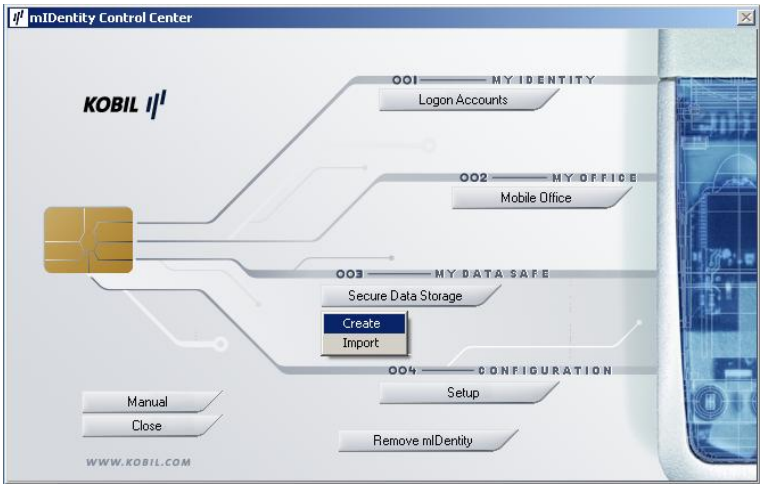

Figure 5.5: Creating a new Secure Data Storage

2. Activate the Checkbox **Secure Data Storage on KOBIL mIDentity**. Please note that only one Secure Data Storage can be stored on KOBIL mIDentity.

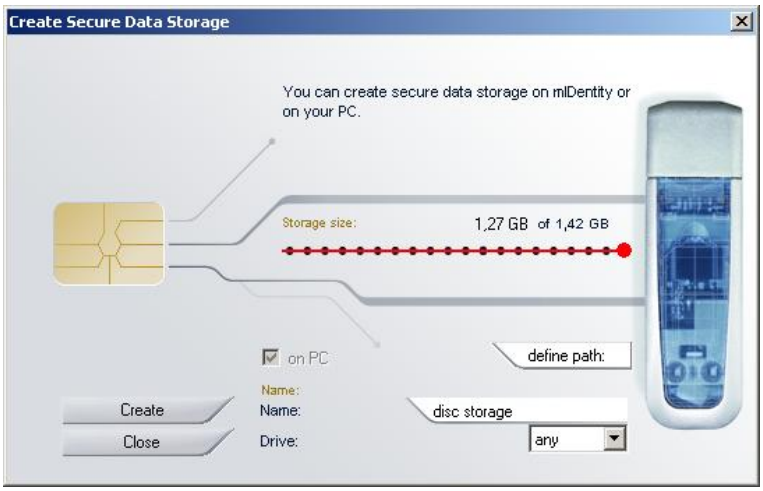

Figure 5.6: Creating a new Secure Data Storage on KOBIL mIDentity

3. Using the slide bar, you can determine the size of the new Secure Data Storage. It can vary between 3 MB and maximum free space on KOBIL mIDentity (depending on the model).

4. Under **Storage Name** you can define a label that will be used to display the Secure Data Storage in the Windows Explorer.

5. You can select a particular **Drive Letter** or ANY, if the Secure Data Storage shall always be mounted to the next available drive letter. A specific drive letter may be useful if you work with scripts.

6. Click **Create** in order to start Secure Data Storage creation. This process may take some time.

7. At the end you have to enter the KOBIL mIDentity SmartCard's PIN to mount and format the Secure Data Storage which completes the process. At the end, the new Secure Data Storage icon appears on the desktop for quick access.

5.2.4 Working with Secure Data Storages

Open the Control Centre Software and click on **Secure Data Storage** in the main window. Select the Secure Data Storage you want to open (logon) or close (logoff).

Depending on the selected Secure Data Storage's state, you can either logon (if it is currently logged off) or logoff (if it is currently logged on).

Local Secure Data Storages stored on your hard disk are marked with a hard disk symbol.

Each time you want to open a Secure Data Storage, you have to enter the KOBIL mIDentity SmartCard PIN - no matter if the Secure Data Storage is stored locally on your hard disk or if it's a mobile Secure Data Storage on your KOBIL mIDentity. After closing the Secure Data Storage, all information is securely encrypted and visible to nobody.

Important: please close all open Secure Data Storages before unplugging KOBIL mIDentity by clicking on "remove mIDentity". If you unplug KOBIL mIDentity without closing Secure Data Storages, data might get lost!

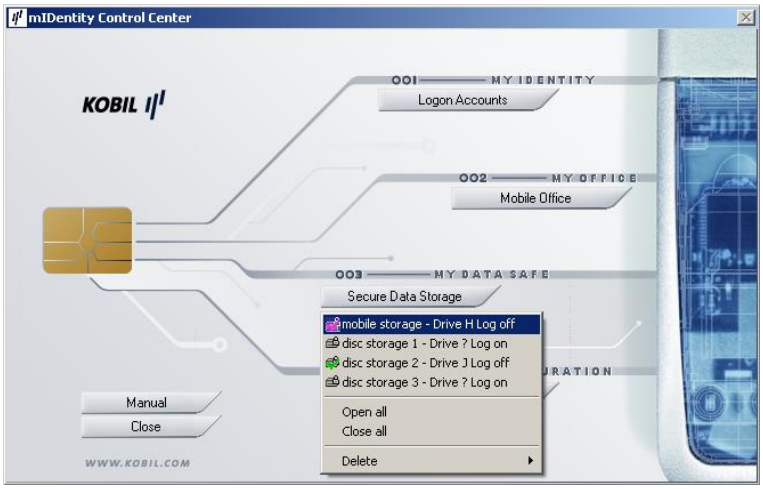

Figure 5.7: Logon / Logoff Secure Data Storages

5.2.5 Delete Secure Data Storages

When you don't need a Secure Data Storage anymore, you can delete it - no matter if it's a local Secure Data Storage on your hard disk or a mobile Secure Data Storage on your KOBIL mIDentity. **Deleting a Secure Data Storage discards all information and files stored in that Secure Data Storage, they cannot be recovered! Be very careful deleting a Secure Data Storage!**

In order to delete a Secure Data Storage, open the Control Centre Software and click on

Secure Data Storage > Delete

and select the Secure Data Storage you want to delete. You will be asked to confirm deletion to make sure that you selected the right Secure Data Storage to be deleted.

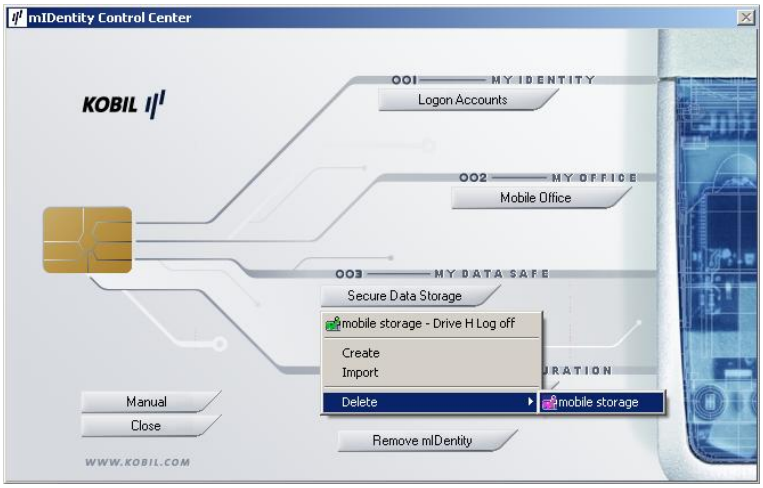

Figure 5.8: Delete Secure Data Storage

5.2.6 Delete a link to a Secure Data Storage

If you have created a Secure Data Storage on a network drive which is currently not available, you can delete the link to this Secure Data Storage. If you do so, the data inside this Secure Data Storage will not be affected. The Secure Data Storage then will only not be recognized from the management software. If the network drive is reachable again you can import the Secure Data Storage and proceed as normal.

In order to delete a link to a Secure Data Storage, open the Control Centre Software and click on

Secure Data Storage > Delete data safe link...

and choose the one, for which the link should be deleted. Then you will be asked to confirm the deletion.

Figure 5.9: Delete Secure Data Storage link

5.3 File Security

KOBIL mIDentity allows you not only to encrypt whole Secure Data Storages, but also single files and directories using digital certificates. The following options are available:

- **Encryption:** Your files are encrypted with a certificate, so that it can only be decrypted using the corresponding private key on your KOBIL mIDentity SmartCard. Only the person owning both the right KOBIL mIDentity can access the file contents. You can encrypt both **files and directories**.
- **Digital Signature:** By means of a digital signature, your data can be protected against unauthorized modification. Furthermore, the data can be assigned to the author. You can sign **files and directories**.
- **Encryption and Signature:** The advantages of encryption and signature are being combined.
- **Secure Erase:** Files and directories are securely erased (deleted) by multiple overwriting.

You can immediately start using file security using the **self-signed certificates** from Secure Data Storage management [7]. This is the easiest way to obtain a certificate, since there is no certificate request at a trust centre needed. But for more comfort, you should apply for a **personal certificate** at a trust centre which allows you to select certificates by user names.

In section 3.4.2, you learn how to obtain such a personal certificate. The following examples show how to work with personal certificates, but the same functionality is available with self-signed KOBIL mIDentity certificates that can be recognized by ther serial number, for example **8949017230000024681**.

5.3.1 File and Directory Encryption

Important: please read carefully section 5.4 before starting to encrypt files or directories in order to keep your data accessible also in emergency situations!

If you want to encrypt a file, proceed as follows:

1. Right-click on the file you want to encrypt. The context menu shown in figure 5.10 appears.
2. Choose

KOBIL mIDentity > Encrypt

[7] your self-signed certificate will be generated as soon as you create the first Secure Data Storage

Figure 5.10: Context menu for file/directory encryption

3. The dialogue shown in figure 5.11 appears. In **Recipients** you see the default encryption certificate (if it is set, see section 5.3.9) and the Additional Decryption Key (ADK, see section 5.4.1). With the **Add** and **Remove** buttons, you can change those settings. Your own certificates are marked with a key symbol, other people's certificates are marked with a certificate symbol.

   Note: depending on the security settings, the administrator can forbid users to remove the ADK certificate from the recipient list in order to enforce ADK usage.

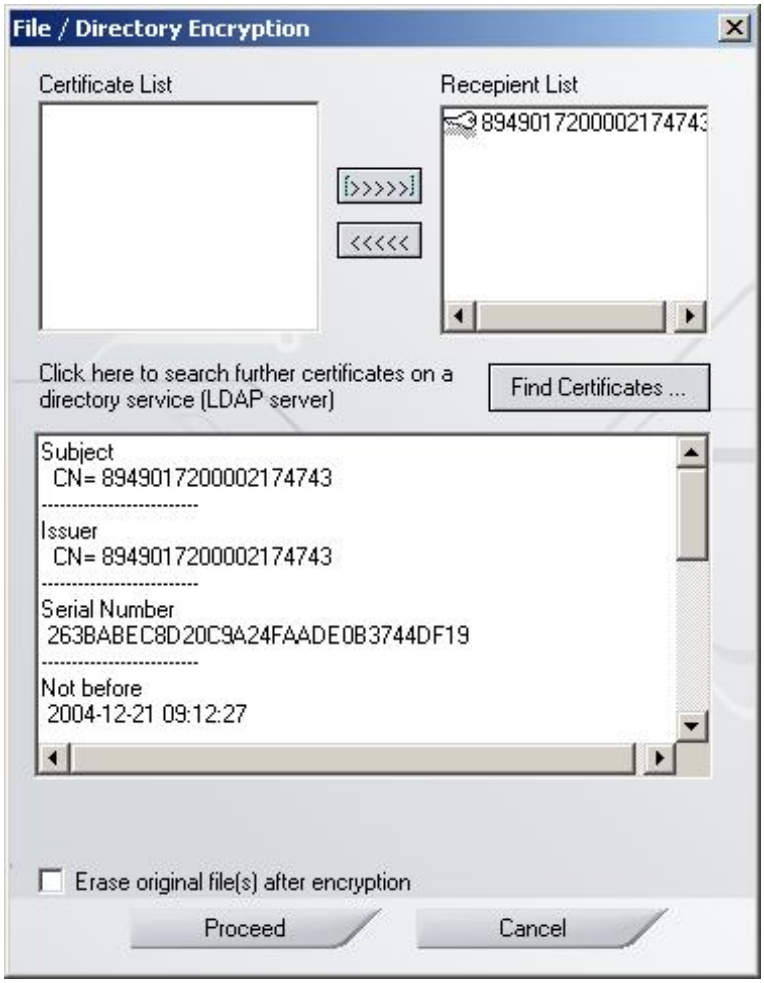

Figure 5.11: File/directory encryption options

The option **Erase original file(s)** determines if the original files will be deleted after encryption. You can define the default setting for that option in the file security preferences (see section 5.3.9).

Warning! If this option is set and you encrypt only to other's people's certificates, you will not be able to read the files anymore!

When all settings are correct, click on **OK** to start the encryption process. An encrypted file will be stored with the file name extension **.kse**, as shown in figur 5.12.

Note: If you want to encrypt files to persons whose certificates are not present locally (they dont appear in the selection list), you can click on **Search** to find the certificate in a directory service as explained in section 5.3.9.

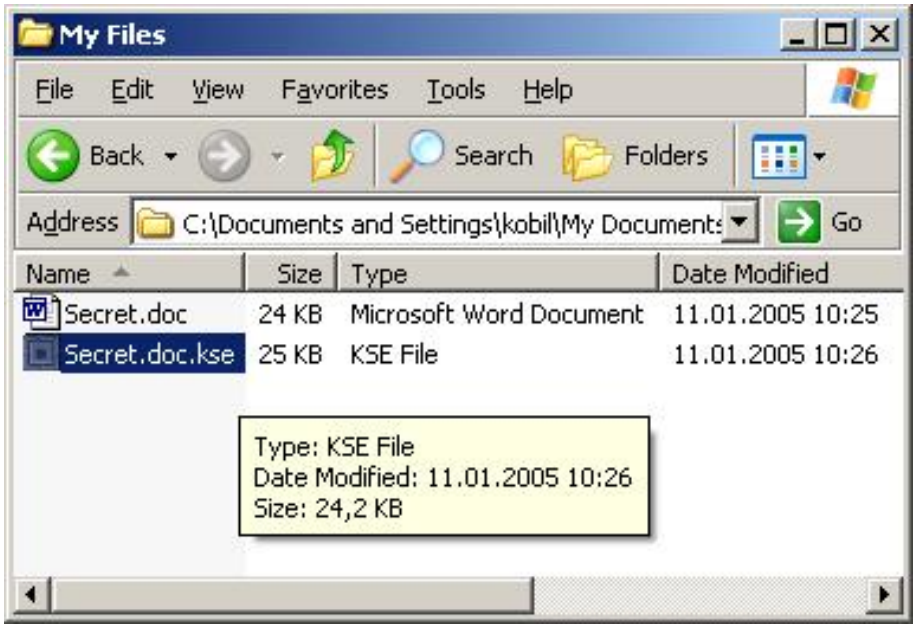
My Files
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Documents and Settings\kobil\My Documents
Go
Name Size Type Date Modified
Secret.doc 24 KB Microsoft Word Document 11.01.2005 10:25
Secret.doc.kse 25 KB KSE File 11.01.2005 10:26
Type: KSE File
Date Modified: 11.01.2005 10:26
Size: 24,2 KB

Figure 5.12: An encrypted file

Encrypted files are stored in PKCS#7 format which enabled interoperability between different applications.

Folder / Directory encryption works exactly as file encryption. Just right-click on the directory you want to encrypt. If you encrypt a directory, all files in that directory will be encrypted in PKCS#7 format, even sub-folders.

You can also add or remove encryption recipients on already encrypted files or directories, see section 5.3.2.

Attention! Never encrypt files necessary for your operating system to start! You may destroy your system configuration!

5.3.2 Add/Remove encryption Recipients

If you want to change the list of encryption recipients of an already encrypted file, right-click that file and select

KOBIL mIDentity > Add/Remove Recipients

Now, the same dialog as for file/directory encryption appears. You can add or remove encryption recipients. After finishing, you will be asked to enter you KOBIL mIDentity's SmartCard PIN, because the file needs to be decrypted before being encrypted to the new recipient list.

Note that you can change the recipient list only if you can decrypt the file, e.g. if your certificate is in the file's current recipient list.

This option is also available for files that are both signed and encrypted (see section 5.3.7).

5.3.3 File and Directory Decryption

You can recognize encrypted files by the ending **.kse**.

1. Right-click on the file you want to decrypt. The context menu shown in figure 5.13 is shown.
2. Choose

KOBIL mIDentity > Decrypt

3. If that file is encrypted with more than one certificate and you have several decryption certificates (or have the ADK registered as an own certificate), you will be asked which certificate shall be used.
4. Enter your KOBIL mIDentity SmartCard's PIN
5. The file is now decrypted and stored without the ending **.kse**.
6. If the encrypted file is deleted after decryption, depends on the preferences (see section 5.3.9).

Alternatively, you can also double-click .kse files. In that case, the file will be decrypted, it will be opened using the appropiate application and after closing the application, the file will be automatically encrypted again (not available for Windows NT).

KOBIL mIDentity also decrypts files that were not encrypted using KOBIL mIDentity if they are in PKCS#7 format and you have the corresponding private key, of course.

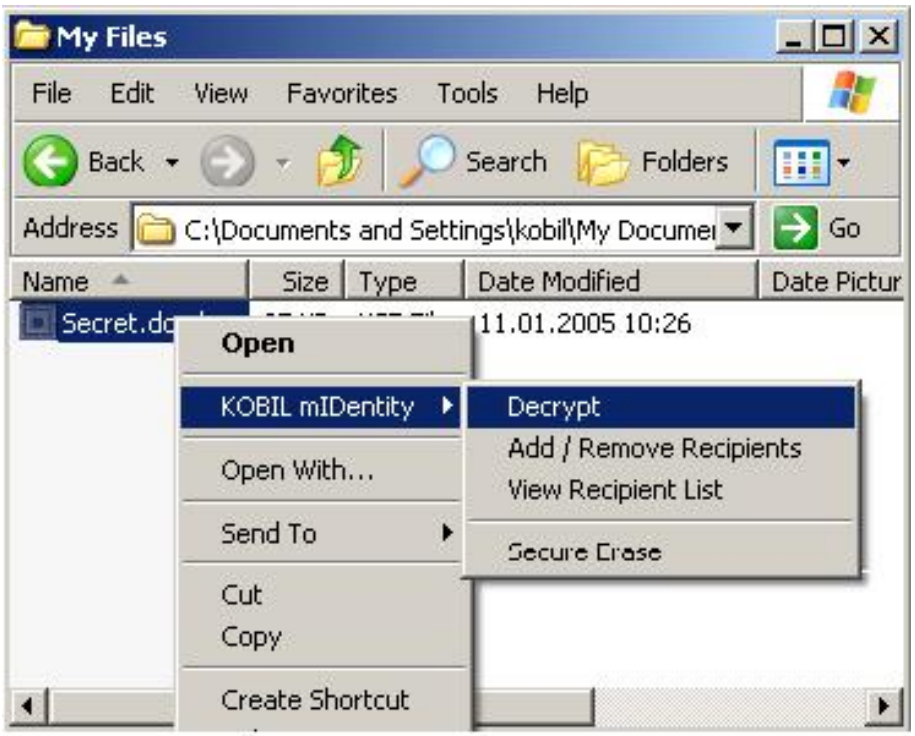

Figure 5.13: Context menu for file/directory decryption

Directory decryption happens exactly the same way as file decryption, just select the directory you want to decrypt with the right mouse instead of a single file. All .kse files in that directory will be decrypted in one pass, but you have to enter your KOBIL mIDentity SmartCard's PIN only once. If not all files in that directory could be processed (either could not be decrypted or not all files are .kse files), you will get a corresponding warning.

5.3.4 File and Directory Signature

Important: this section only covers simple or enhances signatures according to the European Signature Act. If you KOBIL mIDentity version supports qualified signatures, please refer to the section *Qualified Signatures*.

If you want to digitally sign a file, proceed as follows:

1. Right-click on the file you want to sign. The context menu shown in figure 5.14 is shown.

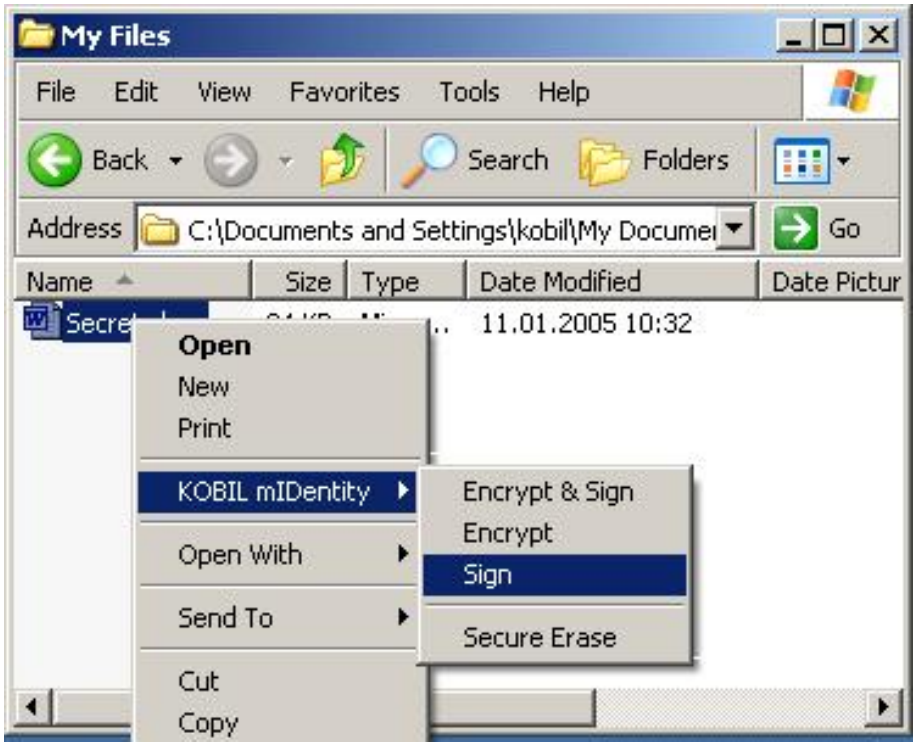

Figure 5.14: Context menu for file signature

2. Choose

KOBIL mIDentity > Sign

3. The dialogue shown in figure 5.15 appears. The following options are available:

   - **Signature Certificate:** This is the default signature certificate configured (see section 5.3.9). If you want to use any other signature certificate, click on **Choose**.
   - **Erase original file(s):** This checkbox decides if the original files should be erased after signature. The default setting of this checkbox can be configured (see section 5.3.9)

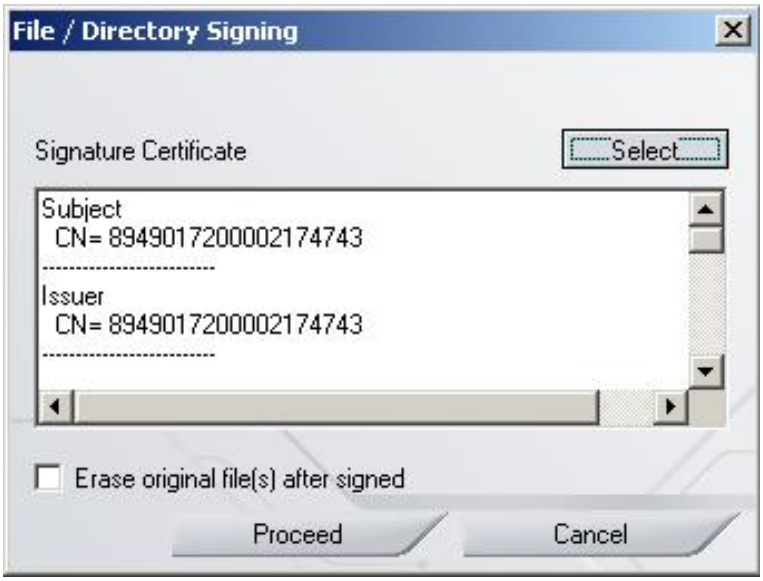

Figure 5.15: File/directory signature options

If all options are correct, click on **proceed** to start the signature process.

4. Enter your KOBIL mIDentity SmartCard's PIN.
5. The file is now signed and stored with the ending **.kss** as shown in figure 5.16.

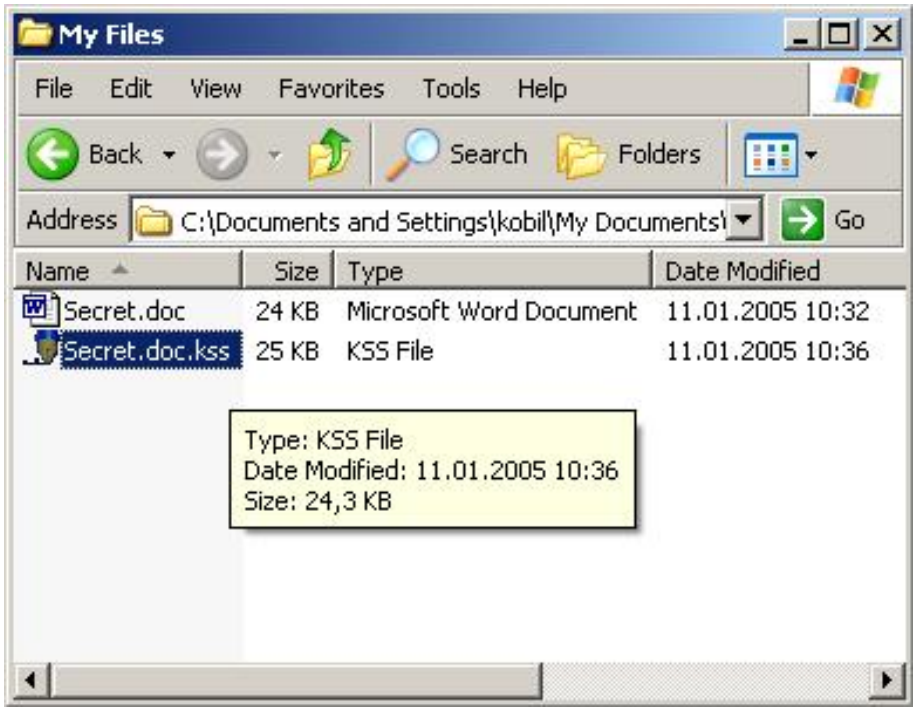
My Files
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Documents and Settings\kobil\My Documents\
Go
Name Size Type Date Modified
Secret.doc 24 KB Microsoft Word Document 11.01.2005 10:32
Secret.doc.kss 25 KB KSS File 11.01.2005 10:36
Type: KSS File
Date Modified: 11.01.2005 10:36
Size: 24,3 KB

Figure 5.16: A signed file

Signed files are stored in PKCS#7 format which enabled interoperability between different applications.

Directory signatures work exaclty the same way as file signatures, just select the directory you want to sign with the right mouse instead of a single file. All files in that directory will be signed (in PKCS#7 format) in one pass, but you have to enter your KOBIL mIDentity SmartCard's PIN only once.

5.3.5 Multiple Signatures

In order to add further signatures to an already signed file, just right-click the .kss file and select

KOBIL mIDentity > Add Signature

As for the first signature, you can select the signature certificate and you will be asked to enter the KOBIL mIDentity SmartCard's PIN.

5.3.6 File and Directory Signature Verification

Important: this section only covers simple or enhances signatures according to the European Signature Act. If your KOBIL mIDentity version supports qualified signatures, please refer to the section *Qualified Signatures*.

To verify a file's digital signature, proceed as follows:

1. Right-click on the file with the ending **.kss** you want to verify. The context menu shown in figure 5.17 appears.

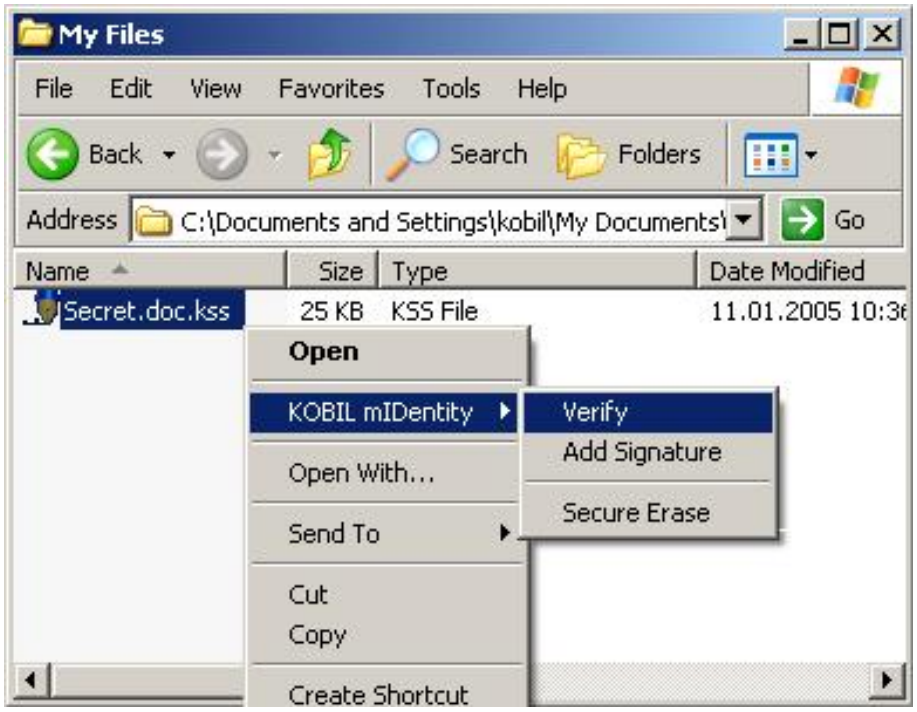

Figure 5.17: Context menu for file/directory signature verification

2. Choose

KOBIL mIDentity > Verify Signature

3. The status dialogue as shown in figure 5.18 appears. In the choice box, you can see the verification status for each file. Click on a file name to see the corresponding signature certificate below.

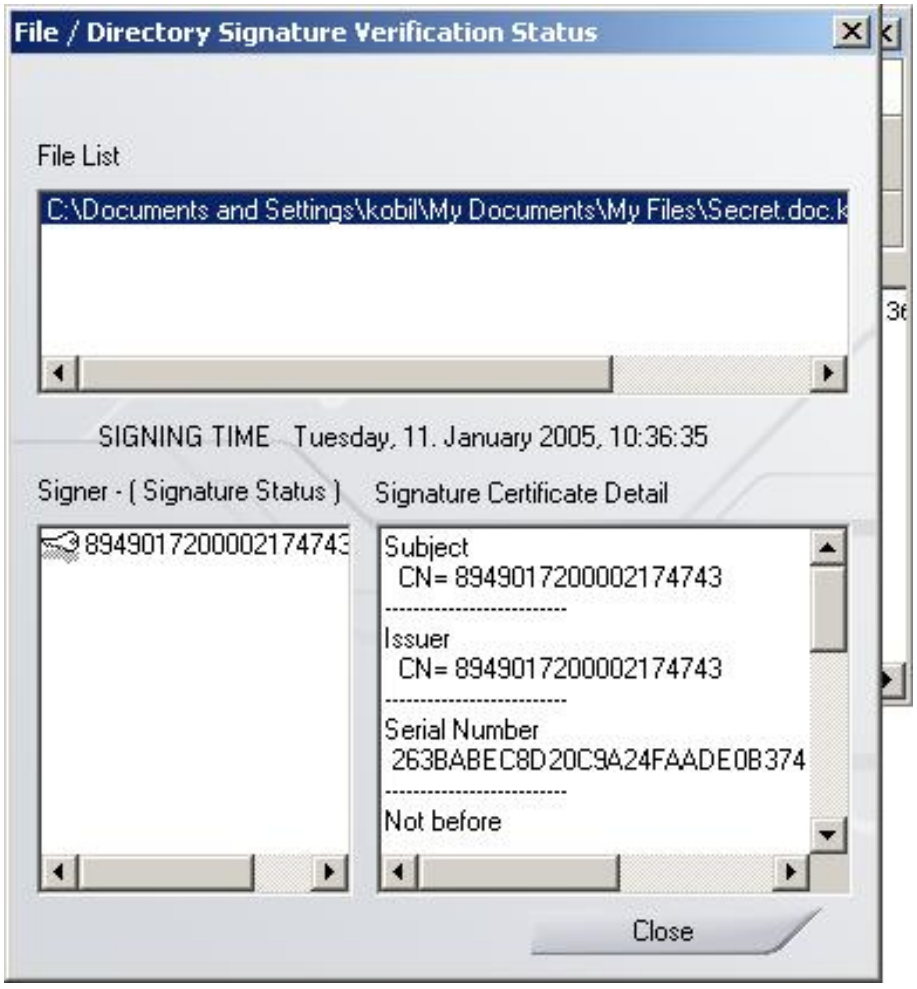

Figure 5.18: Signature Verification Status

4. All verified files are stored without the ending **.kss** in a new file. If the signature file (with the ending **.kss**) is deleted or not, depends on the configuration as described in section 5.3.9.

Signature verification for directories works exactly as for single files. Just select a directory you want to verify with the right mouse. All signed (.kss) files in that directory will be extracted (original files without signature) and at the end of the process, the verification status for all files will be displayed. If not all files in that directory could be processed (e.g. not all files are .kss files), you will get a corresponding warning.

5.3.7 Signature and Encryption of Files and Directories

Important: please read carefully section 5.4 before starting to encrypt files or directories in order to keep your data accessible also in emergency situations!

If you want to encrypt and sign a file or a directory in one step, proceed as follows:

1. Right-click on the file or directory you want to encrypt and sign. The context menu shown in figure 5.19 appears.

2. Choose

KOBIL mIDentity > Encrypt & Sign

Figure 5.19: Context mennu for file/directory signature and encryption

3. The dialogue shown in figure 5.20 appears. The following options are possible:

   - **Signature Certificate:** This is the default signature certificate (see section 5.3.9). If you want to use any other signature certificate, click on **Choose**.
   - **Recipients:** This is the default encryption certificate (see section 5.3.9) and - if set - also the ADK certificate (see section 5.4.1). If you want to use any other encryption certificate, click on **Add**. You can also **Search** for other people's certificates in directory services.
   - **Erase original file(s):** This checkbox decides if the original files should be erased after encryption/signature. The default setting of this checkbox can be configured (see section 5.3.9) **Attention! If this checkbox is active and you are about to encrypt to a foreign certificate, you will not be able to recover those files!**

   If all options are correctly set, click on **proceed** to start the encryption/signing process.

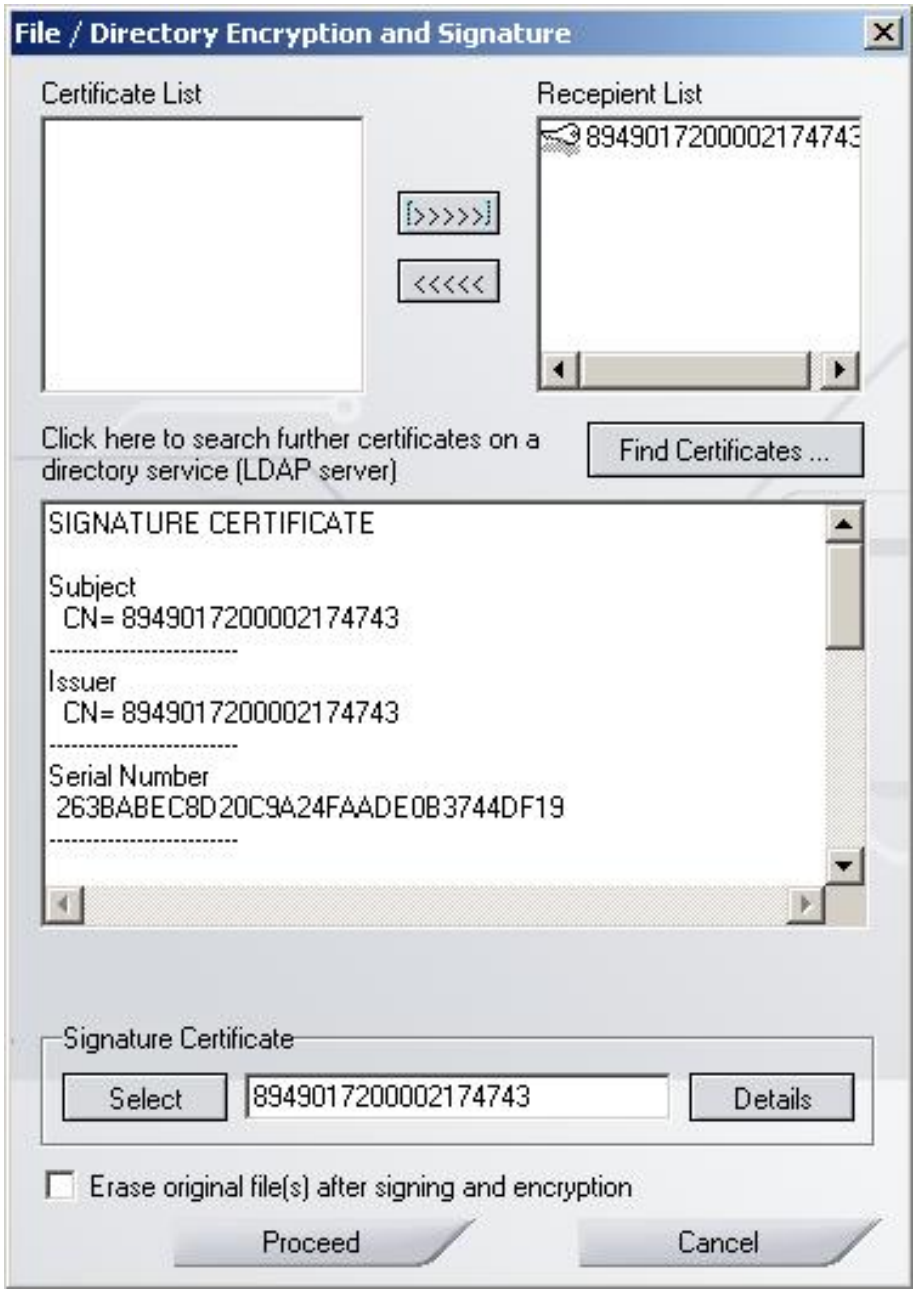

Figure 5.20: File/directory encryption and signature options

4. Enter your KOBIL mIDentity SmartCard's PIN.
5. The file (e.g. all files inside the chosen directory) are now encrypted and signed and stored with the ending **.ksk** as shown in figure 5.21.

My Files
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Documents and Settings\kobil\My Documents\
Go
Name Size Type Date Modified
Secret.doc 24 KB Microsoft Word Document 11.01.2005 10:4
Secret.doc.ksk 26 KB KSK File 11.01.2005 10:4
Type: KSK File
Date Modified: 11.01.2005 10:44
Size: 25,0 KB

Figure 5.21: A signed and encrypted file

Encrypted and signed files are stored in PKCS#7 format which enabled interoperability between different applications.

Attention! Never encrypt files necessary for your operating system to start! You may destroy your system configuration!

5.3.8 Signature Verification and Decryption of Files and Directories

Signed and encrypted files have always attached the ending **.ksk** in their name. If you want to decrypt and verify the signature of a file or a directory in one step, proceed as follows:

1. Right-click on the file or directory you want to decrypt and verify. The context menu shown in figure 5.22 appears.
2. Choose

KOBIL mIDentity > Decrypt & Veriy

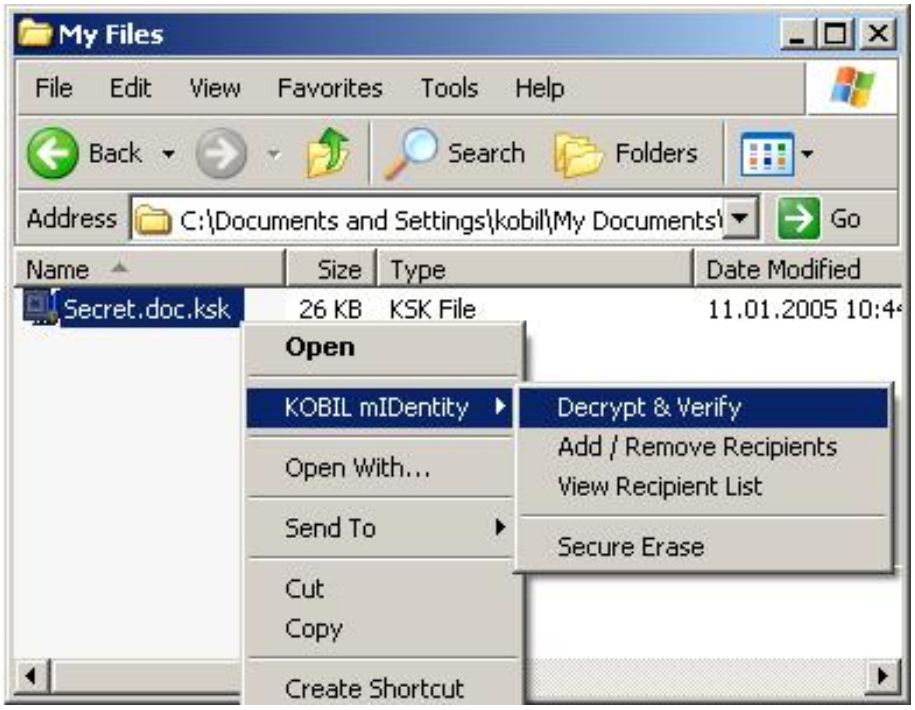

Figure 5.22: Context mennu for file/directory signature verification and decryption

3. Enter your KOBIL mIDentity SmartCard's PIN.
4. The file (e.g. all files inside the chosen directory) are now decrypted and verified and stored without the ending **.ksk**. The signature verification result is shown as in figure 5.18. If not all files in that directory could be processed (either could not be decrypted or not all files are .ksk files), you will get a corresponding warning.

5.3.9 Default Settings for File Security

Open the Control Centre Software and select

Setup > Secure Data Storage

and choose the drawer **File Security**.

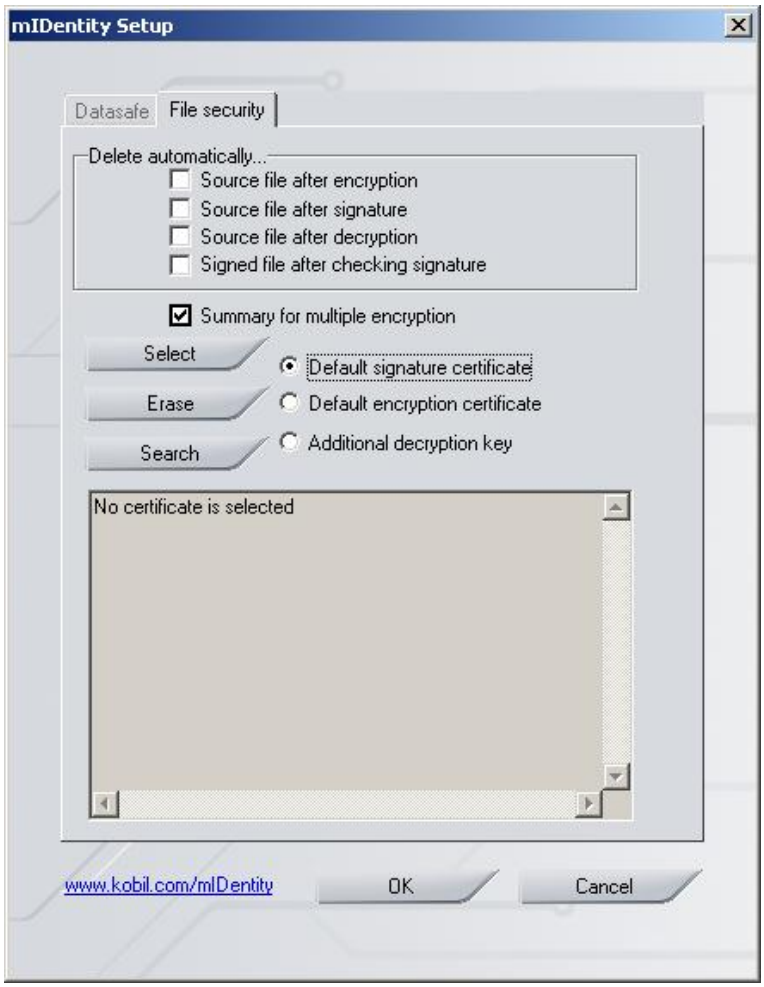

Figure 5.23: File Security Settings

For getting more detailed information please visit http://www.kobil.com and download the KOBIL mIDentity whitepaper wich will answer your questions.

Erase Options

- If the checkbox **Original files after encryption** is active, each original file is deleted automatically after encryption. You can change this behaviour also per encryption process (see sections 5.3.1) and 5.3.7).
- If the checkbox **Original files after signing** is active, each original file is deleted automatically after signature. You can change this behaviour also per signature process (see section 5.3.4).
- If the checkbox **Encrypted files after decryption** is active, each encrypted file is deleted automatically after decryption. **Note that this option cannot be changed per decryption process!**
- If the checkbox **Signed files after signature verification** is active, each signed file is deleted automatically after signature verification.
  Note that this option cannot be changed per signature verification process!

Show Report after Process

If you enable this option, you will see a report about how many files have been processed in case you selected multiple files or even complete folders to encrypt, decrypt, sign, verify or secure erase.

Default Signature Certificate

Check *Default Signature-Certifikate* and click on *Select*. You can select the default signature certificate from the list of all valid signature certificates (see section 5.3.4). The button *Remove* disables the default signature certificate.

Important: this setting does NOT have any impact on *qualified signatues*

Default Encryption Certificate

Check *Default Encryption-Certifikate* and click on *Select*. You can select the default encryption certificate from the list of all valid encryption certificates (see section 5.3.1). The button *Remove* disables the default encryption certificate.

Additional Decryption Key

Check *Additional Decryption Key* and click on *Select*. You can select the Additional Decryption Key from the list of all valid encryption certificates. The button *Remove* disables the Additional Decryption Key.

Important: Please read section 5.4.1 carefully before changing Additional Decryption Key configuration!

Important: An ADK certificate has only impact on file and directory encryption, NOT on e-mail encryption!

Search Certificates

Using this button, you open a search dialogue that allows you to look up other people's certificates stored in so-called *directory services* and store them in your local Windows certificate store. This is a very useful function if you often encrypt files to other people.

Directory services are managed by Outlook and Outlook Express. If you don't want to use one of the pre-configured directory services, you should configure your individual directory service first, as described in section 3.4.5

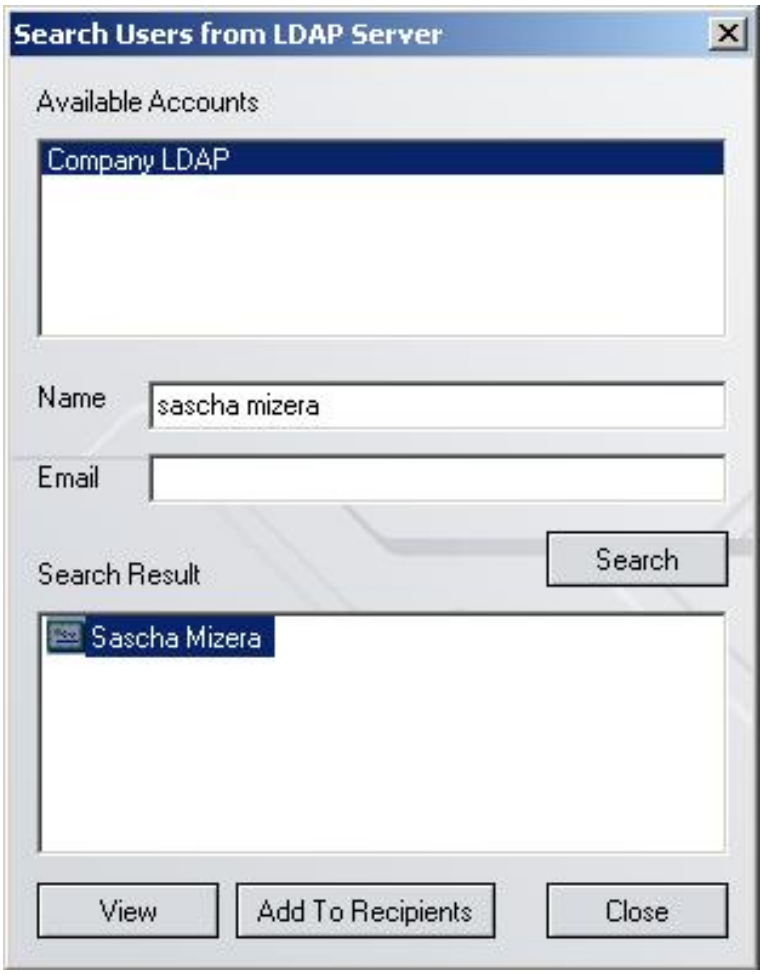

Figure 5.24: Search Certificates

The dialogue shown in figure 5.24 shows all directory services configured in Outlook and Outlook Express. You can search for the person's name or email address. If one or more results have been found, you can show them and import them into the Windows certificate manager where they will be displayed in *Other People* as described in section 3.4.3.

Note:
If you want to search for user certificates in Active Directory, please configure a new directory service account for Active Directory first as described in section 3.4.5. As server name, please enter the domain controller's full DNS name. The search base must be written in the so-called "DC-notation". Example: if your domain is called "myDomain.myCompany.de", the DC notation will be "dc=myDomain, dc=myCompany, dc=de".

5.4 Emergency Recovery

5.4.1 Additional Decryption Keys

The cryptograhpic mechanisms used in KOBIL mIDentity are so strong that nobody can recover the encrypted text without knowledge of the corresponding private key. Your private key is well-protected on your KOBIL mIDentity SmartCard. But it can of course happen that you lose your KOBIL mIDentity or it is stolen. As the KOBIL mIDentity SmartCard is PIN-protected, nobody can gain unauthorized access to your data.

To make those data accessible for yourself in such a case, KOBIL mIDentity supports so-called *Additional Decryption Keys, ADK*. Using Additional Decryption Keys, every Secure Data Storage, file and directory you encrypt with your certificate is also encrypted with another configurable certificate that we call *Additional Decryption Certifikate*.

Each Additional Decryption Certificate of course also has a corresponding private key. This private key needs not to be located on a SmartCard. Depending on your security policy, the Additional Decryption private key is kept in a secure place like a bank tresor. It is not needed during normal operation.

In case where a file cannot be decrypted anymore because the corresponding private key is temporarily or forever unaccessible, it can still be decrypted using the Additional Decryption private key. To do so, the file must be present on a machine where KOBIL mIDentity installed and where the Additional Decryption is registered – either on another KOBIL mIDentity or as a software certificate. In case of a software certificate you have to import it on your KOBIL mIDentity before using it. Please refer to section 3.4.6.

Should it be necessary to use the Additional Decryption Key on another SmartCard in your KOBIL mIDentity, proceed as follows: After inserting the KOBIL mIDentity (with new SmartCard, which contains the new Additional Decryption Key) you will be called upon to enter the card-PIN for the Simple Sign-On solution. Since only your secure data storages are encrypted with the ADK certificate and not the passwords please cancel the PIN entry, otherwise an error message will occur. After confirming the error message you can access the decrypted data (except of passwords) anyway.

Attention! Additional Decryption Keys are not used for e-mail encryption!

Please refer to section 5.3.9 how to configure the ADK certificates.

Chapter 6

Your mobile Office

In this section, you learn how to use KOBIL mIDentity to secure your daily digital communication.

6.1 Secure Email Communication using Outlook & Outlook Express

In this section, you'll learn how to secure your e-mails using Microsoft Outlook Express, 98 and 2000/xp/2003 with KOBIL mIDentity.

We assume that both your internet access and e-mail account are properly configured. If you are not sure about this, contact your internet provider.

Email security functions can be combined with Outlook Synchronization (see section **??**.

Before starting to sign and encrypt emails, you need a **personal certificate** that contains your email address. Self-signed certificates cannot be used for secure email communication since they dont contain an email address. See section 3.4.2 how to get a personal certificate.

6.1.1 Configure your Certificate

To send signed messages and receive encrypted messages, you have to configure your e-mail certificate. If you don't select a default certificate and try to send a signed message, Outlook Express prompts you with a list of certificates to choose from. The "big" Outlook versions dont allow to send secured email unless you have configured your certificate manually.

The necessary steps differ a bit between Outlook Express and Outlook 98/2000/xp/2003

Outlook Express

In Outlook Express, your certificates are bound to your e-mail account, so you can select a default certificate for a each account.

1. Start Outlook Express and select

   Tools > Accounts

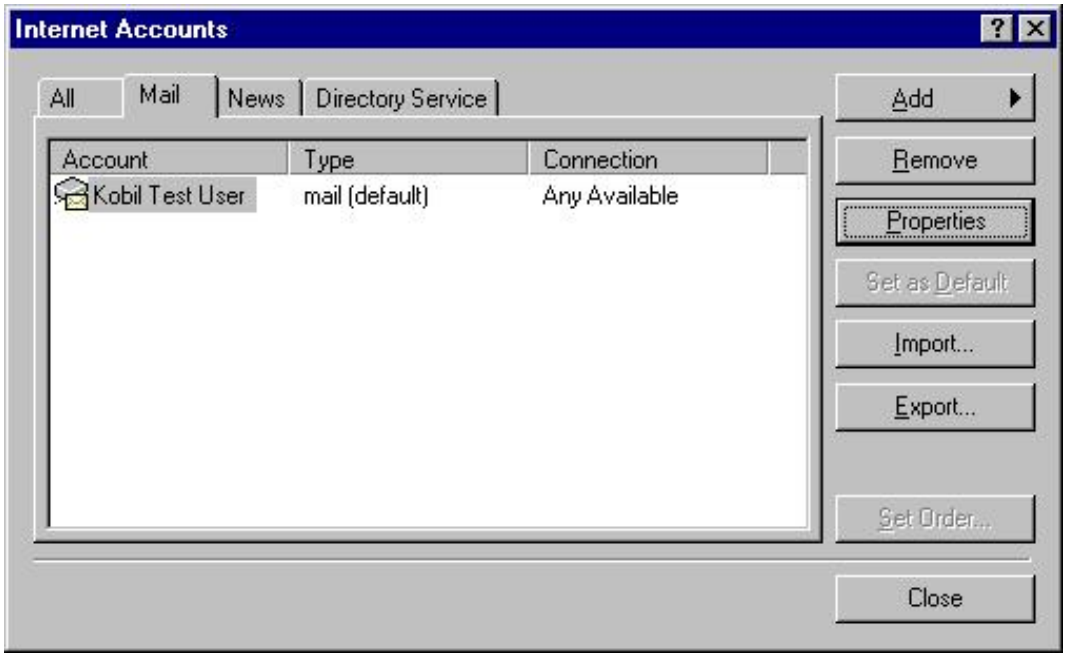

Figure 6.1: Internet Accounts Dialog

2. Choose your e-mail account as shown in figure 6.1 and click

   Properties > Security

   The dialogue shown in figure 6.2 will appear.

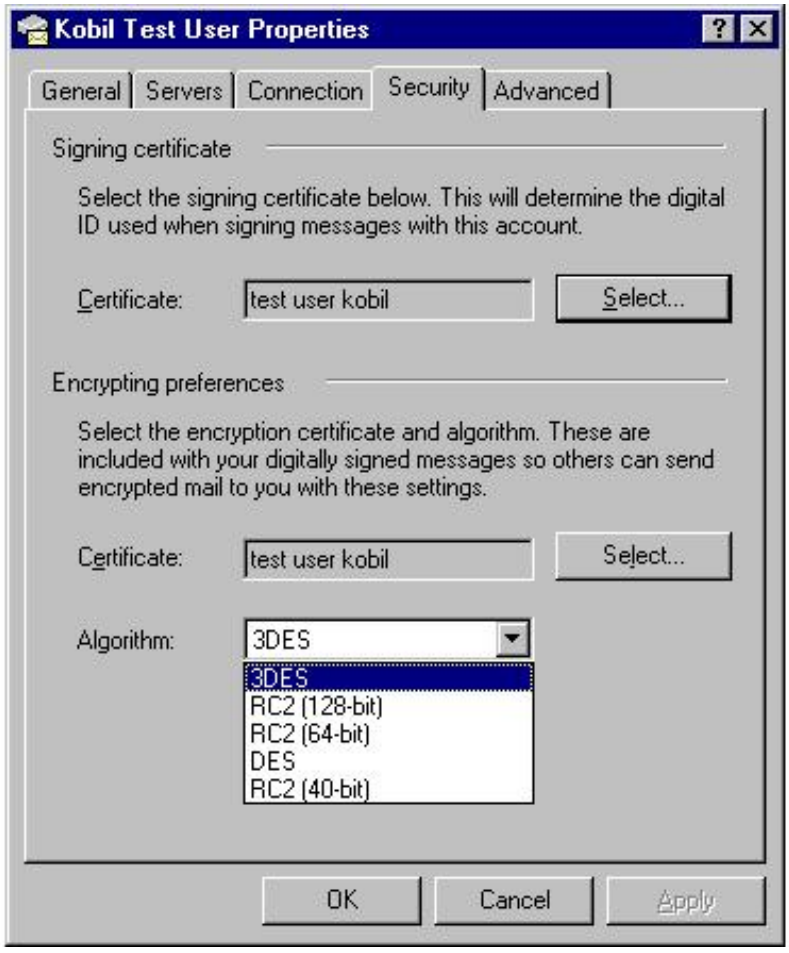

Figure 6.2: Internet Accounts properties Dialog

3. Click **Select** and choose a certificate from the list that shows all the certificates which can be associated with the account you selected above. If there are other certificates which don't have the same e-mail account information, they will not be displayed in this list. You can select the same certificate for signature and encryption if your security policy allows this. The dialogue is shown in figure 6.3.

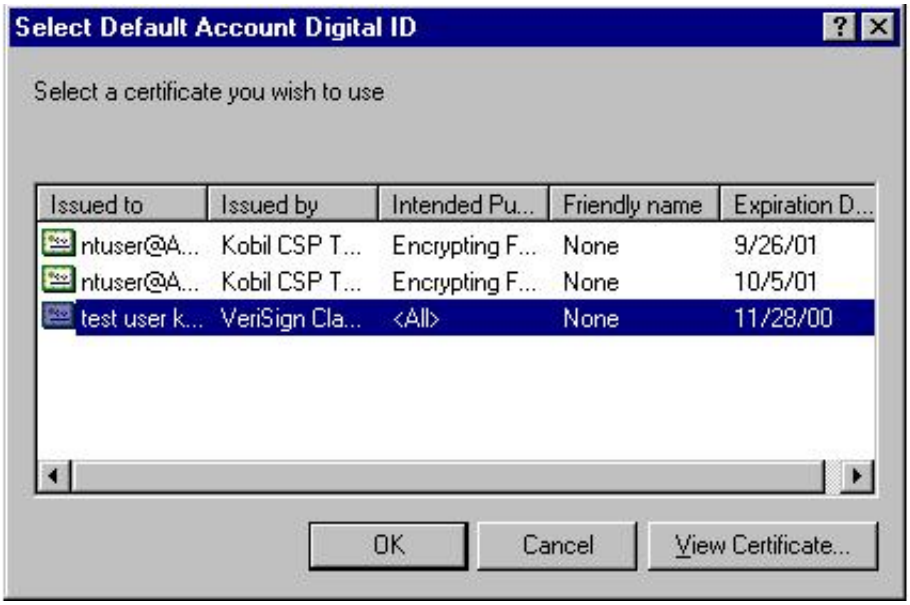

Figure 6.3: Select Digital ID Dialog

4. You can select the session key algorithm which will be used for bulk encryption and decryption. For strongest security, **3DES** or **RC2 128-bit** is recommended.

Outlook 98 / 2000 / xp / 2003

1. Start Outlook and choose the menu

   Extras > Options

2. Choose the drawer **Security** as shown in figure 6.4.

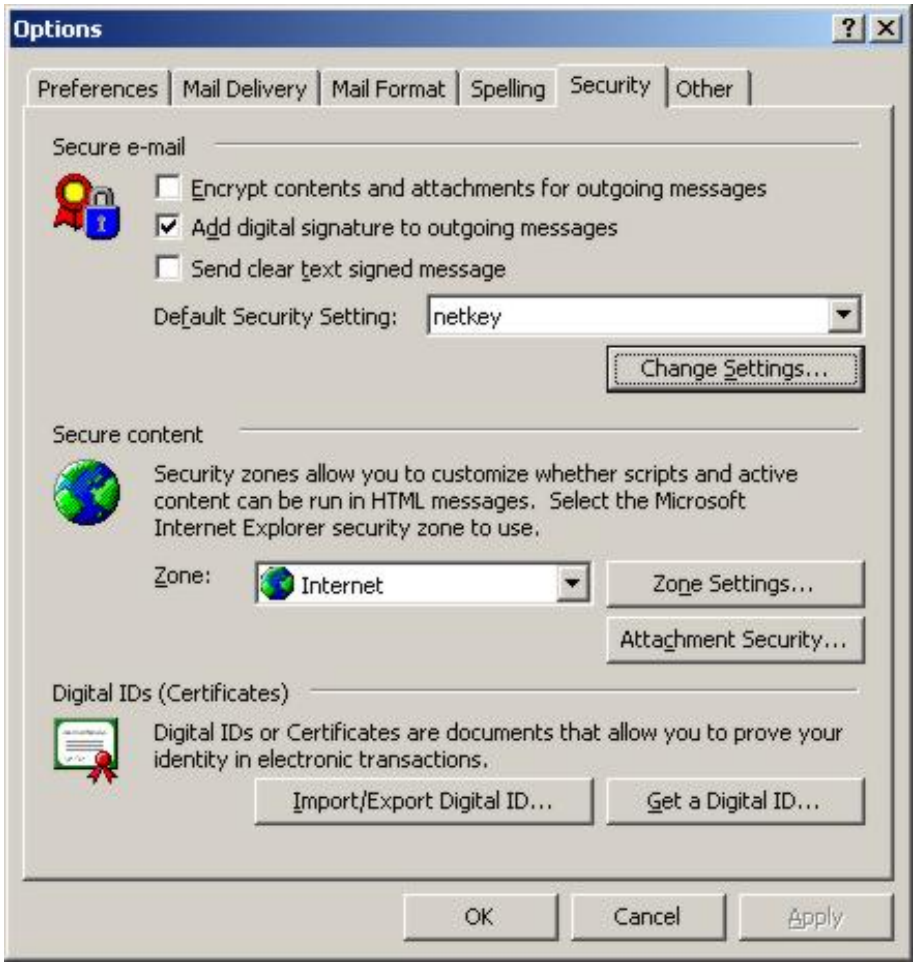

Figure 6.4: Security Options dialogue in Outlook 98 / 2000 / xp / 2003

3. Click on the button **Change Settings...**. The dialogue shown in figure 6.5 will appear.

4. You can now select two independent certificates for signature and encryption using the **Choose...** buttons. **Be careful to select a certificate which contains the e-mail address suitable for your e-mail account!** You can select the same certificate for signature and encryption if your security policy allows this. The dialogue is shown in figure 6.3.

5. You can select the session key algorithm which will be used for bulk encryption and decryption as well as the hashing algorithm for digital signatures. For strongest security, **3DES** or **RC2 128-bit** is recommended as encryption algorithm and **SHA1** as hashing algorithm.

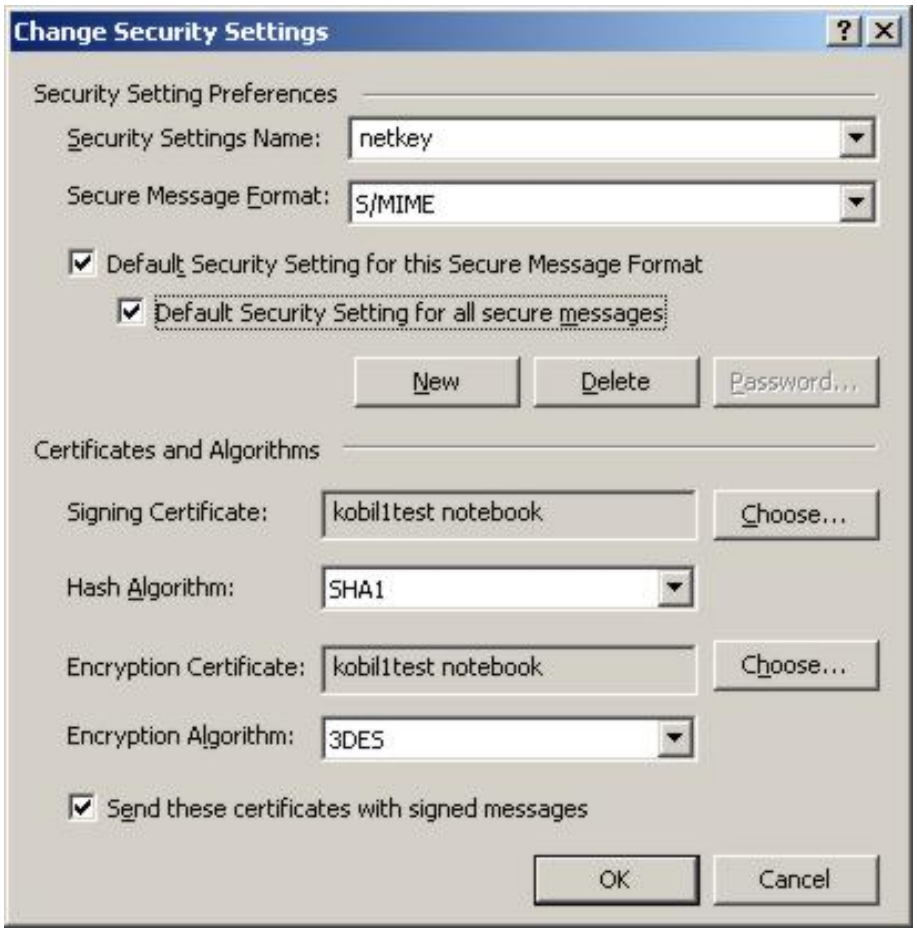

Figure 6.5: Outlook 98 / 2000 / xp / 2003 certificate selection

6.1.2 Setting up Outlook Security Buttons

In order to comfortably sign and encrypt your emails, you can set-up the appropriate Outlook buttons.

Outlook Express

In Outlook Express, the buttons are already present but they are that much outside the window, they are hidden. To make them visible, proceed as follows:

1. Open a new email

   File > New > EMail Message

   A new email window is opened

2. Choose the menu

   View > Menu Bar > edit

3. The buttons **Sign** and **Encrypt** can be found under **current buttons**. Mark them and move them towards the beginning of the menu using the arrow-up button until they become visible.

Outlook 98 / 2000 / xp / 2003

By default, the "big" Outlook versions hide the buttons. To activate them, proceed as follows:

1. Open a new email message using the menu

   File > New > EMail message

   A new email window is opened

2. Choose the menu

   View > Menu Bar > edit

3. Choose the drawer **Commands** and select the category **Standard** on the left side.

4. In the selection field **Commands:** you find them at the end: **sign message content and attachments** and **encrypt message contents**. Drag-and-drop them with the left mouse button to the menu bar.

6.1.3 Sending secure Email

To send a secure email, proceed as follows:

1. Write your email as usual. If you add attachments to the email, they will also be signed and/or encrypted.

2. If you want to **digitally sign** the email, activate the button **Sign Message**, as shown in figure 6.6 (Outlook Express). If the button is not visible, please refer to section 6.1.2 to configure it.

3. If you want to **encrypt** the email, activate the button **encrypt message contents** as shown in figure 6.7 (Outlook Express). If the button is not visible, please refer to section 6.1.2 to configure it.

4. You can combine encryption and signature.

5. Send your email as usual using the **Send** button.

6. If the email is to be signed, you will be asked to enter the KOBIL mIDentity SmartCard's PIN to enable the private key for signing.

If the email will only be encrypted (not signed), step 6 (PIN entry) is omitted, since the private key is not needed for encryption.

It may be that Outlook complains about a **missing recipient certificate**, which is necessary to encrypt the email. In this case, you can look it up using a directory service. Please refer to section 3.4.5 to learn how to configure and use a directory service.

You can configure your default settings to sign and encrypt all outgoing messages (Click **Tools** > **Options** > **Security** and place checkmarks). If you do not define a default behaviour for signing and encryption, you can use **Sign** and **Encrypt** buttons of the new mail window.

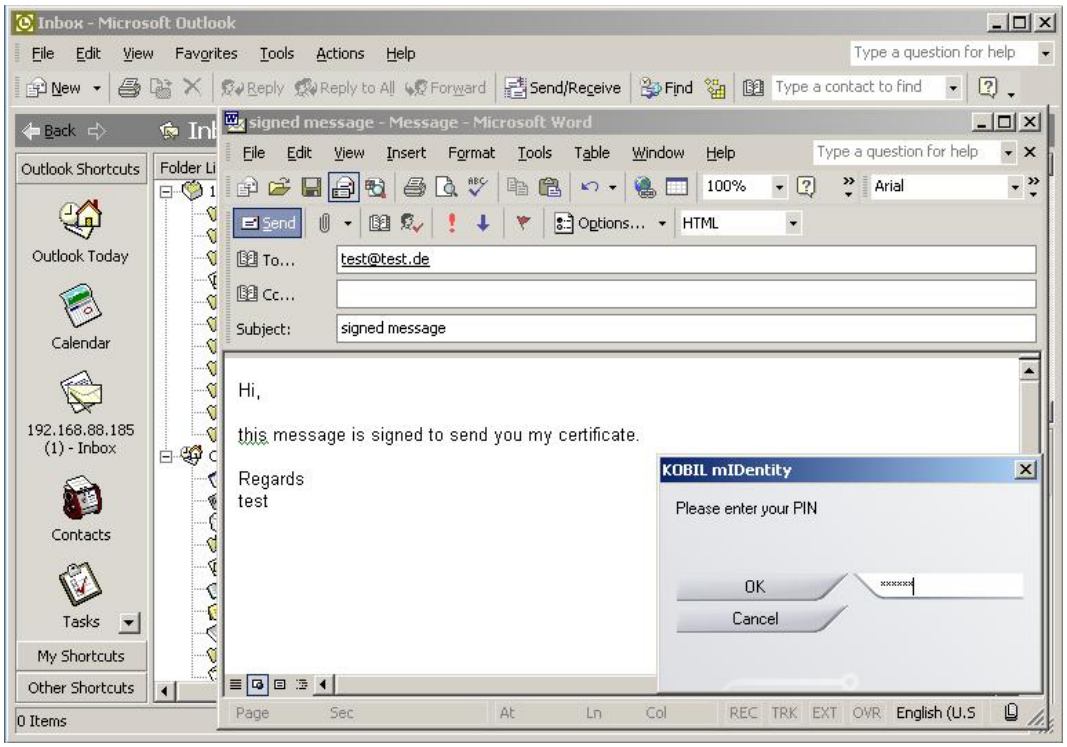

Figure 6.6: Digital Signature using Outlook Express

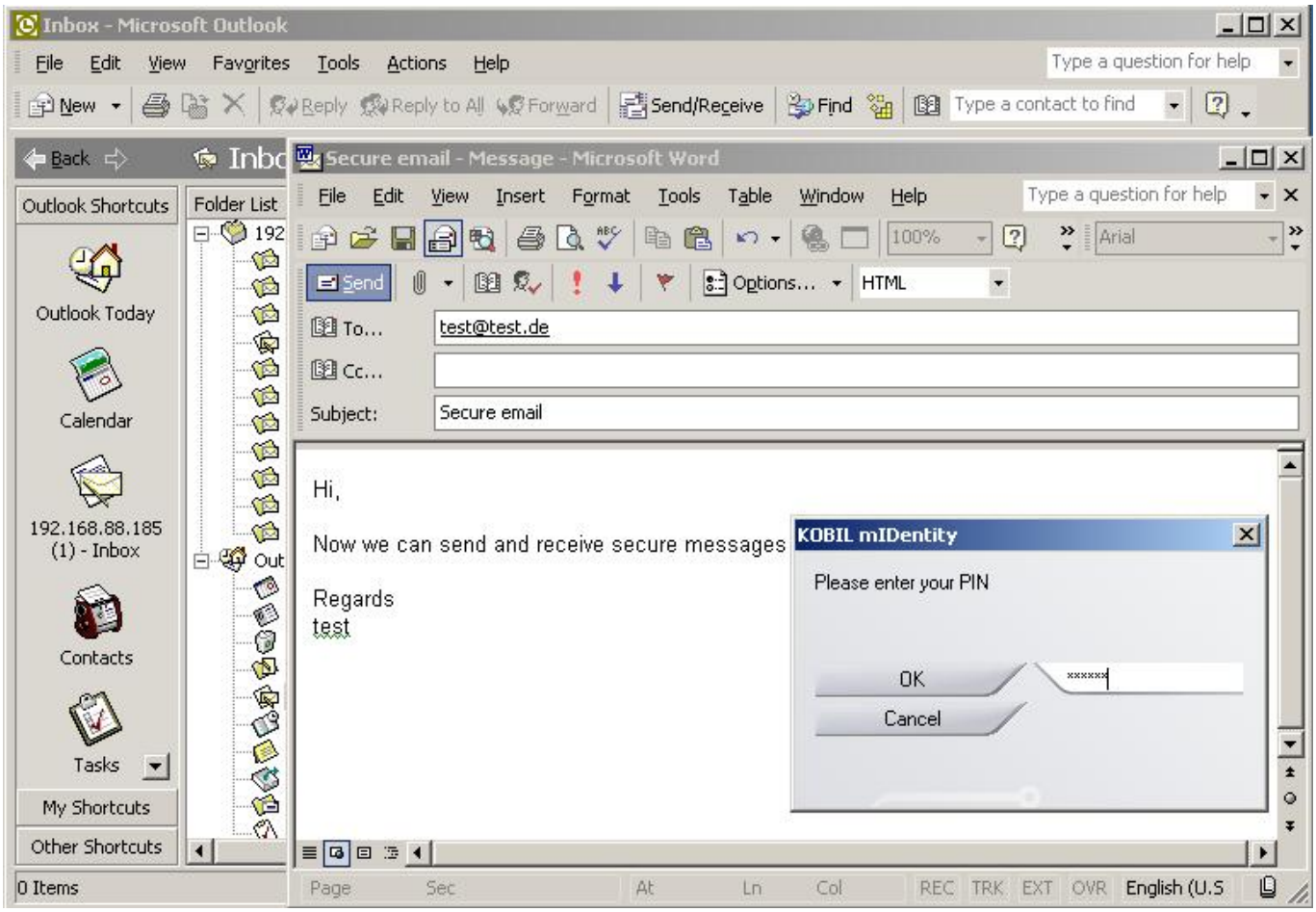

Figure 6.7: Encrypted and signed Email using Outlook Express

6.1.4 Receiving secure E-mail

If you receive a signed email, it is marked with a red rope symbol (see figure 6.8). Click on that symbol to verify the signature and watch the signer certificate.

When receiving an encrypted email, you will be asked to enter your KOBIL mIDentity SmartCard's PIN in order to decrypt the email's content. Encrypted emails are marked with a blue lock symbol as shown in figure 6.9). Click on that symbol to see the encryption strength and encryption certificate.

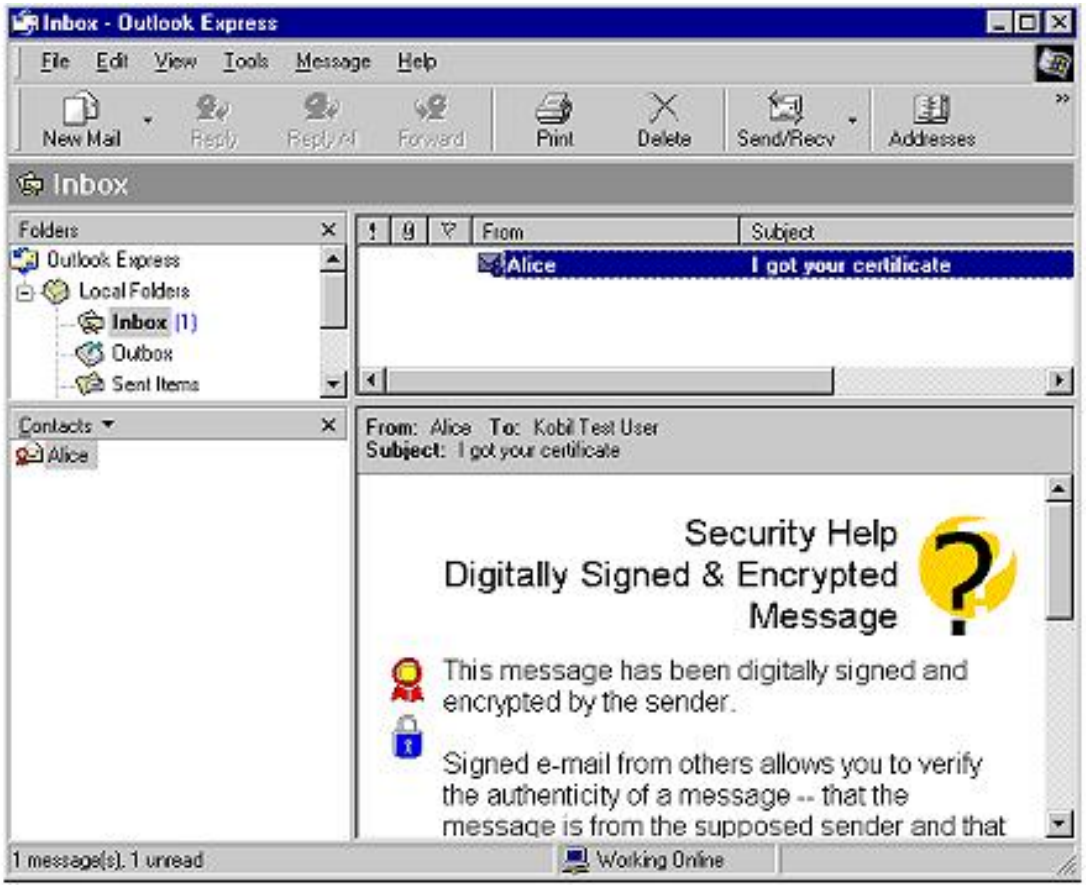
Inbox - Outlook Express
File Edit View Tools Message Help
New Mail Reply Reply All Forward Print Delete Send/Recv Addresses
Inbox
Folders
Outlook Express
Local Folders
Inbox (1)
Outbox
Sent Items
From Subject
Alice I got your certificate
Contacts
Alice
From: Alice To: Kobil Test User
Subject: I got your certificate
Security Help
Digitally Signed & Encrypted Message
This message has been digitally signed and encrypted by the sender.
Signed e-mail from others allows you to verify the authenticity of a message -- that the message is from the supposed sender and that
1 message(s), 1 unread
Working Online

Figure 6.8: Receiving a signed email with Outlook Express

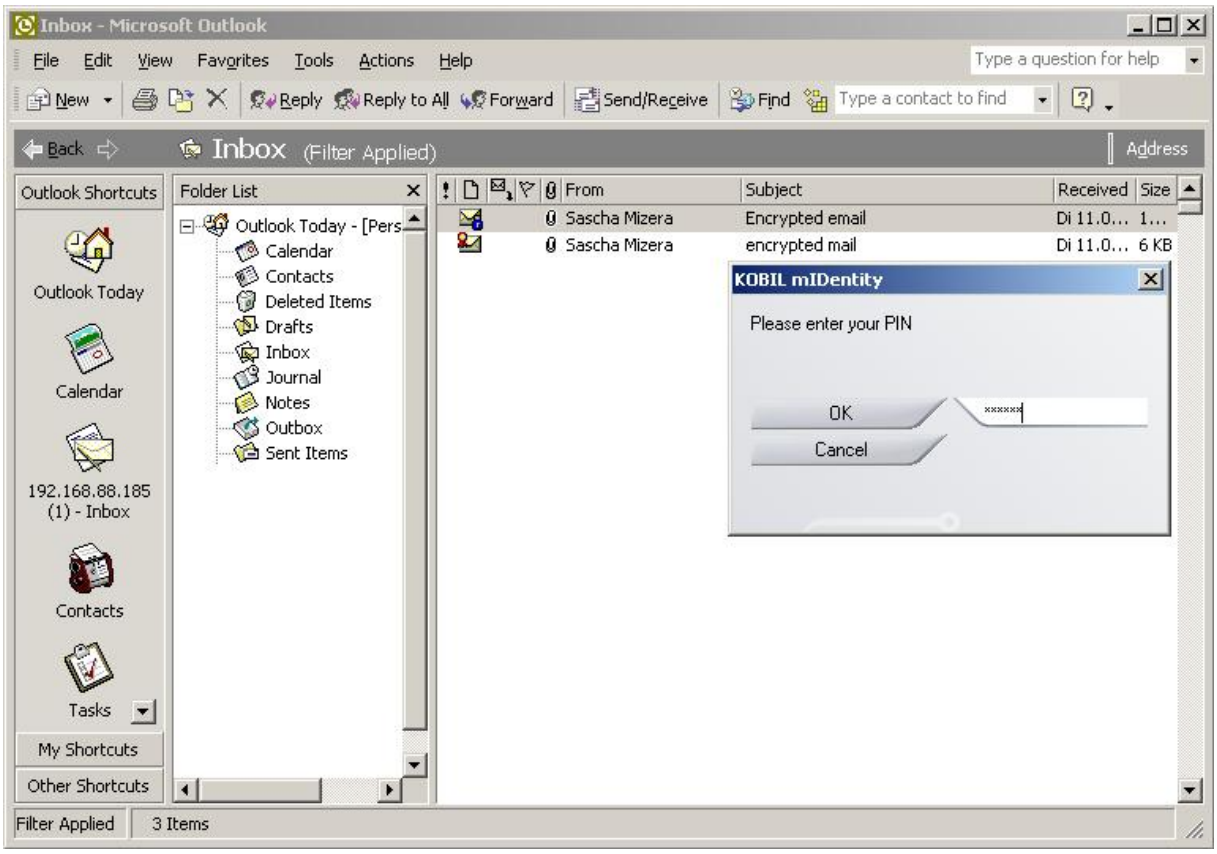

Figure 6.9: Receiving an encrypted email with Outlook Express

6.2 KOBIL eSecure für SAP R3

If you are interested in the optional KOBIL eSecure for SAP R3 support please contact your certified KOBIL partner.

Appendix A

Cryptographic Basics and Standards

A.1 Security Objectives

Confidentiality Protection from disclosure to unauthorised persons who may try to listen to communication or to steal some information.

Integrity Maintaining data consistency. Nobody except the originator can change the information while it is stored somewhere or transfered in an insecure media like the Internet.

Authentication (Non-repudiation / Access control) Assurance of identity of a person or an originator of data. The originator of some data cant deny it later. Unauthorized persons are kept out.

A.2 Terms and Basics

Cryptography is the science of keeping information secure. Cryptographic systems usually consist of two implemented processes: encryption and decryption.

Encryption is the process of transforming a message (the plaintext) into another message (the ciphertext) such that it is computationally infeasible to derive the plaintext data by reversing the process without knowledge of secret parameters. Many cryptographic algorithms mathematically combine input plaintext data and an encryption key to generate ciphertext data.

Decryption is the reverse process of encryption and transforms the ciphertext data back into the original plaintext data by using a complex function and a decryption key. One of the goals of cryptography is to raise the cost of guessing the decryption key beyond what is practical. The algorithm type and the key length are the most important measures against predictability of the key.

Cryptography has nothing to do with obscurity. Cryptographic algorithms and protocols should be conform with standards to support interoperability. Using non-published algorithms is contraproductive to compatibility. Moreover, cryptography is not about hiding algorithms, but it is about designing strong algorithms and secure mechanisms. Security and interoperability must both be achieved in years by building and testing very well-known algorithms, mechanisms and protocols. Security should be obtained only by storing the keys in a secure way and by making algorithms so strong that they are impractical to break.

A.3 Standards

A.3.1 Data Digestion Algorithms

Data Digestion Algorithms are not used for encryption or decryption. The main purpose of these algorithms is to produce a unique "fingerprint" (typically 16 or 20 bytes in length) of the original data.

Digestion algorithms are also called "one-way hash functions", because it is computationally infeasible to recover the original data from its digest or even to find some other data which will produce the same digest. Ideally, each digest is unique and every bit is influenced by every bit of its input data. These algorithms are used together with other types of algorithms to supply digital signature processes (see below). The most common digestion algorithms are MD5, RipeMD and SHA1. Figure A.1 illustrates the data digestion process.

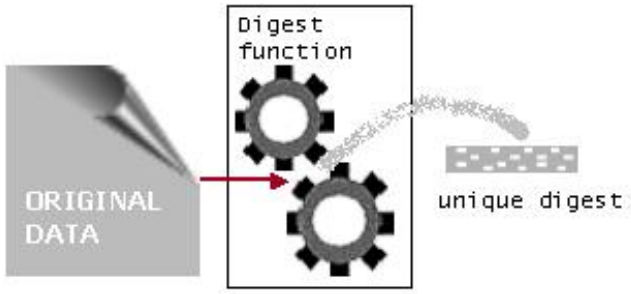

Figure A.1: Data Digest scheme

A.3.2 Symmetric Encryption Algorithms

With these type of algorithms, the same key (the so-called "session key") is used to encrypt and the decrypt the message. They are also known as "session key algorithms". Figure A.2 illustrates the symmetric encryption process.

The main advantage of symmetric algorithms is their speed of data encryption and decryption. The main weakness is the key management. Both sender and receiver must have the same secret session key which must be transferred securely. It is convenient and secure to transfer session keys by using public key algorithms. The most common session key algorithms currently are triple DES, RC2 and RC4.

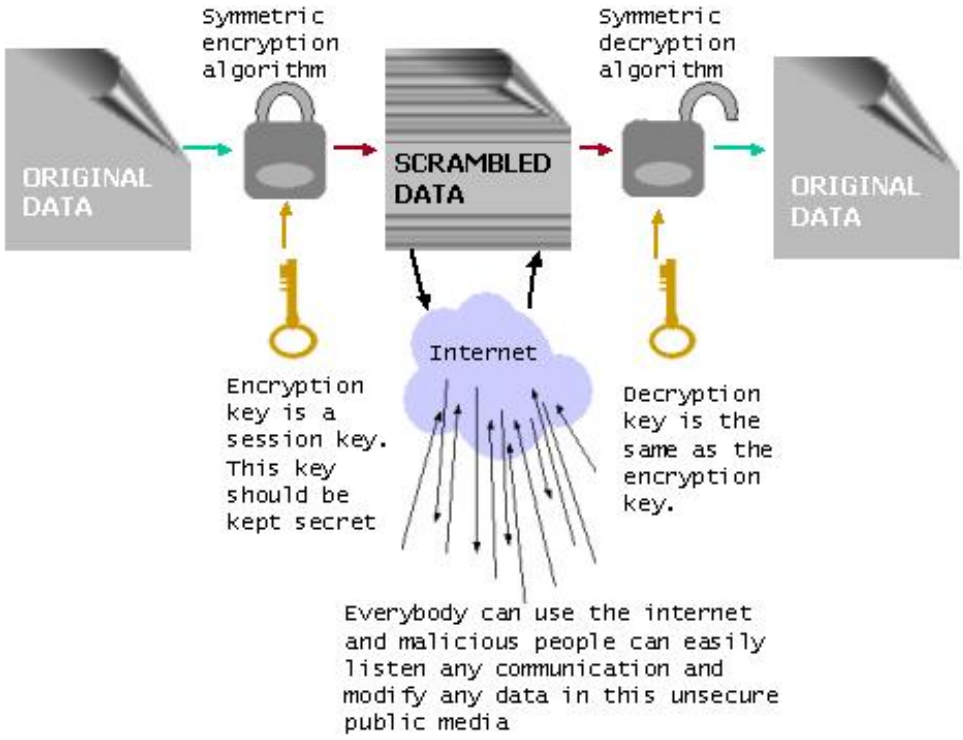

Figure A.2: Symmetric Algorithm

A.3.3 Public Key Algorithms

Properties

With these algorithms, encryption and decryption keys are different. Each user has at least one key pair consisting of two keys. One is kept secret, so it is called a "private key", and the other one is open, which is called "public key". Private keys are unique for each user and they are never transferred to other people.

If someone needs to send a data to you, he needs your public key. He encrypts data with your public key and no one except you can decrypt the scrambled data using your private key. The transfer (or distribution) of your public key is secured by the help of "trusted authorities". Such a trusted authority will provide you a certificate for your public key. This means that they provide a packet of data containing both your public key and the trusted authority's assurance that this is really your public key. Figure A.3 illustrates the usage of public key process for a secure data transfer.

The main advantage of the public key algorithms is the secure key distribution. Their main disadvantage is the slow processing speed for encryption and decryption of large data. Because of this slowness, public key algorithms are used with together with symmetric session key algorithms to supply the necessary speed. To support confidentiality, public key algorithms are used to wrap and unwrap the session keys (for a secure session key transfer). To support both integrity and authentication, public key algorithms are used to sign and verify the output of data digestion algorithms. The most common public key algorithm is RSA.

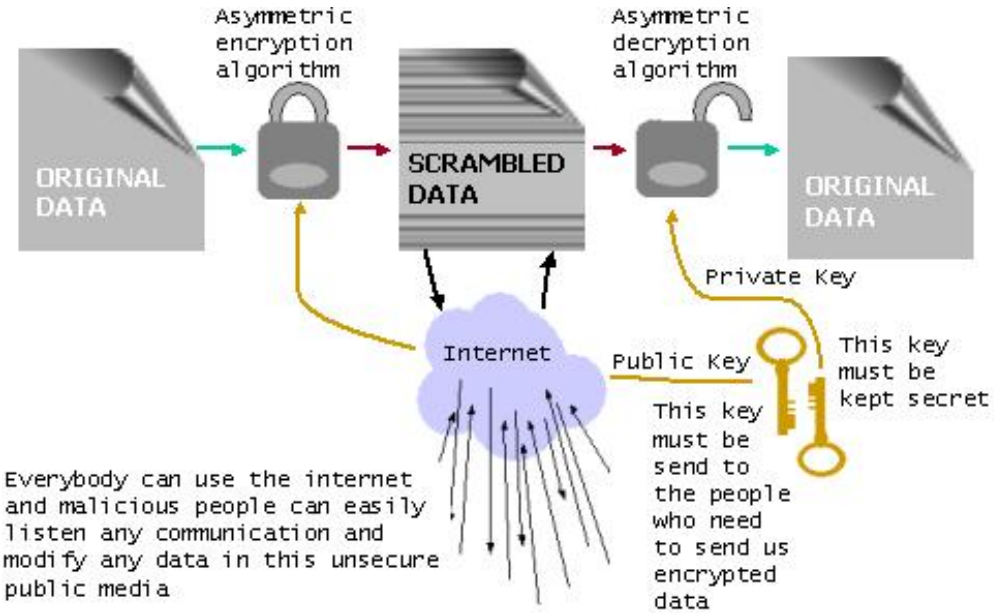

Figure A.3: Asymmetric Algorithm

Wrap Session Key

Bulk data is encrypted with a session key to supply fast speed. The encryption session key must be sent to the recipient for decryption. For a secure transfer, the session key is encrypted with the public key of the recipient. No one except the recipient can recover the session key, because the private key of the recipient is needed to decrypt the scrambled session key. Encrypted bulk data and the scrambled session key are merged to form a digital envelope. Someone who wants to recover the original data must recover the session key first (see figure A.4).

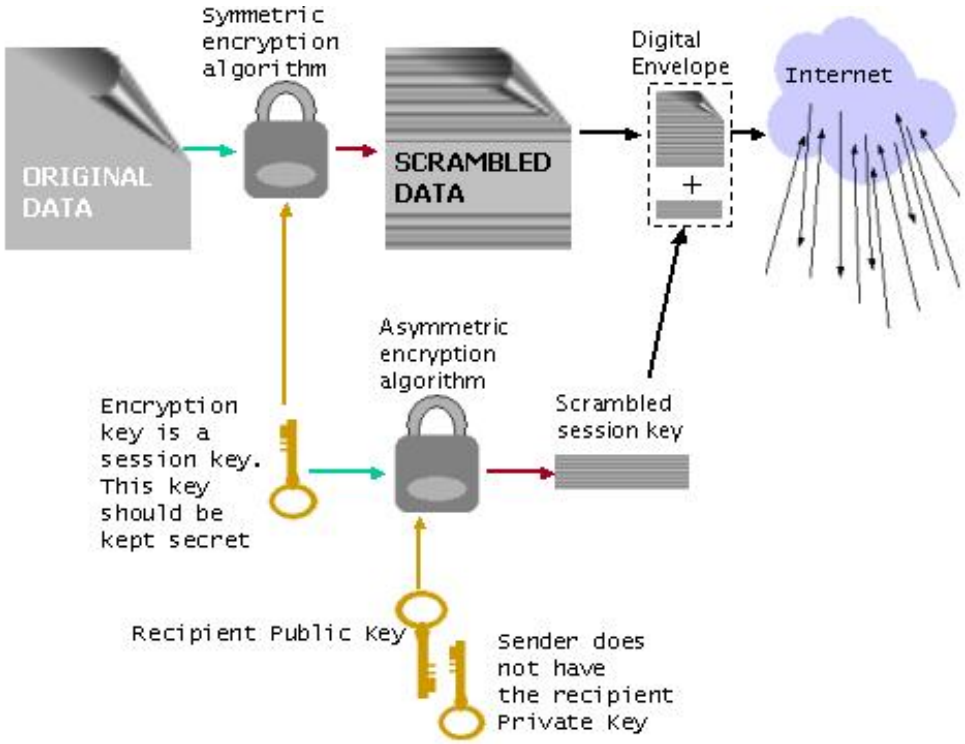

Figure A.4: Wrap Session Key

Unwrap Session Key

The recipient of the digital envelope detaches the scrambled session key from the encrypted bulk data. First, the scrambled session key is decrypted with the private key of the recipient. Second, bulk data is decrypted with the recovered session (decryption) key as shown in figure A.5.

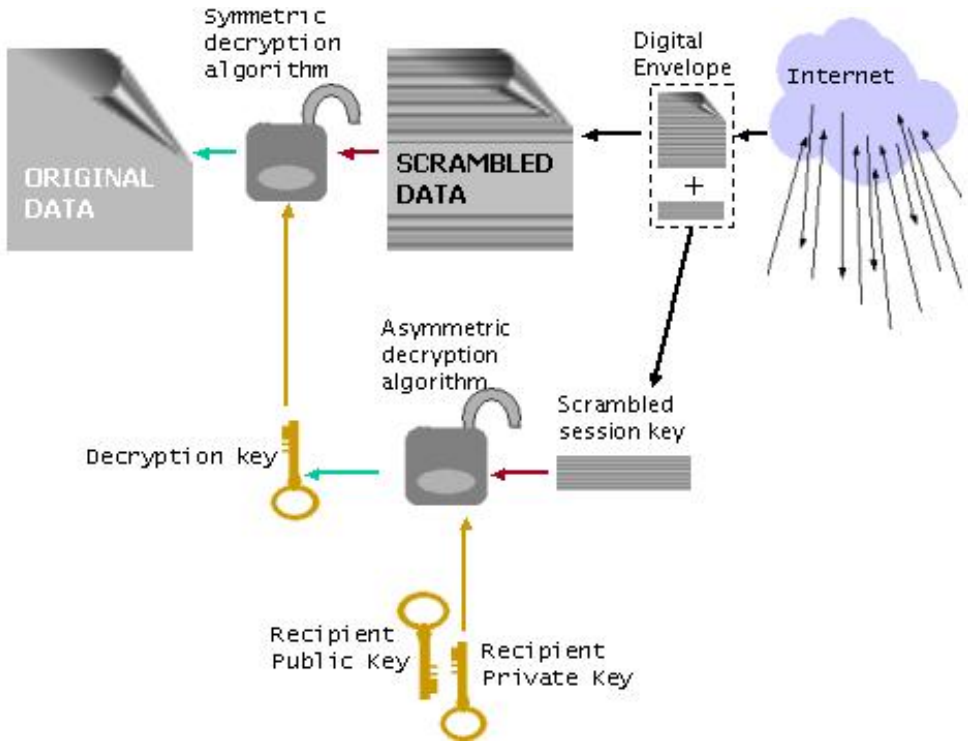

Figure A.5: Unwrap Session Key

Digital Signatures

Digital signatures are needed for the authentication of identities. A digital signature binds an individual to unique data. That's why there are two inputs of the signing process: first, the data itself and second, the private key of the signing individual.

Digestion algorithms are used to reduce the size of the bulk data because of the slowness of the public key algorithms. First, the message is digested and then the unique digest is encrypted with the originator's private key. Output is the signature. Anybody can decrypt this signature, because anybody can get the corresponding public key of the sender. The result of decryption is the unique digest and it is practically infeasible to find another message with the same digest.

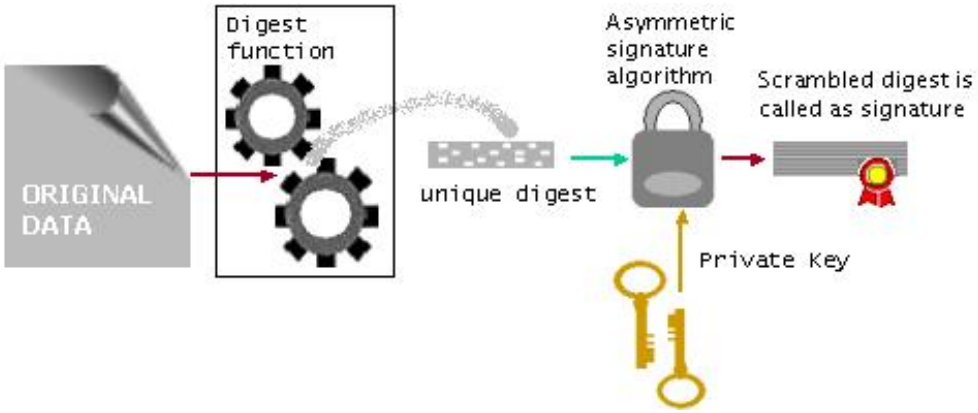

Figure A.6: Signature Creation

Verification of Digital Signatures

To verify a digital signature, someone needs both the signature and the input data. A recipient of the signature decrypts it with the sender's public key to recover the data digest. The recipient also digests the input data to get the original data digest. If the recovered data digest is the same as the original digest, the signature is correct. Otherwise, the sender is not the person who he claims to be or the original data was modified on its way. Digital signatures support both authentication and integrity. For confidentiality, digital signing process is combined with the encryption process of session keys and the wrap operation of public keys.

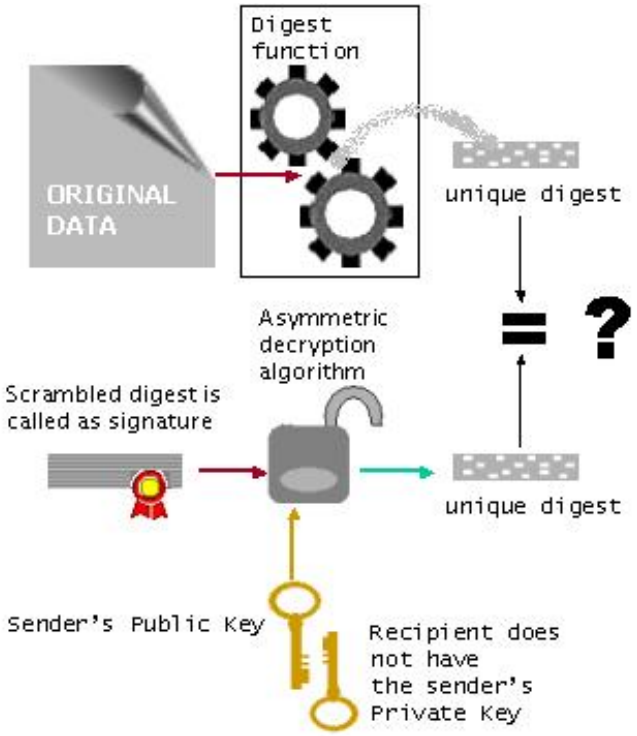

Figure A.7: Signature Verification

A.3.4 Digital Certificates

A certificate is a set of data that includes a public key and other owner- specific information to identify an entity. The certificate owner has the corresponding private key. Certificates are issued by certification authorities (CA) which are trusted organisations. Each certificate is protected by a signature that is created by a CA. Certification authorities and certificates make public key distribution secure. Secure storage and usage of a certificate and its corresponding private key is the problem of its owner. KOBIL Smart Key helps certificate owners with this problem by presenting a hardware based security system that uses SmartCards.

The most widely accepted standard for digital certificates is defined by International Telecommunications Union's ITU-T X.509 standard. A X.509v3 certificate includes the following data fields:

- Version
- Certificate's serial number
- Signature algorithm ID
- Issuer name
- Expiration date
- User name
- User public key information

- Issuer unique identifier (optional)
- User unique identifier (optional)
- Extensions (optional, contain certificate usage instructions)
- Issuer's signature over the fields above

A.3.5 Certificate Authorities

A certificate authority (CA), also called "trust centre", is a trusted organisation that issues public key certificates. A CA acts as a guarantor of the binding between the subject's public key and the subject's identity information that is contained in the certificates it issues.

The typical process of getting and using a certificate goes something like this (the user is called *Alice*[1] in this example):

1. Alice creates a cryptographic key pair, consisting of a private and a public key.
2. Alice creates a certificate request that contains her name, her public key, and perhaps some additional information.
3. Alice signs her certificate request with her new (corresponding) private key.
4. Alice sends the signed request to a CA.
5. The CA creates a data set from Alice's request.
6. The CA signs the data set with its private key.
7. The CA forms a certificate with the data set and its signature.
8. The CA returns the certificate to Alice who is now the owner of the certificate.

To give a real meaning to this process, the CA would of course need to make sure that Alice really is Alice (and not e.g. Bob claiming to be Alice). This however causes additional costs and actions in real life, so this is something which a pure Internet service cannot provide. However, there are companies offering that type of service.

Today's most popular browsers and e-mail programs know the certificates of very well known and more or less trusted CAs. So people can easily verify the signatures of many CAs. This helps people to decide whether a certificate and its content is trustworthy or not. If a certificate is signed and issued by an unknown CA and your browser does not have the public key of that CA, then your browser gives a warning and asks whether to proceed or not.

The typical certificate distribution and verification between users:

1. Alice sends her certificate to Bob to give him access to her public key. This is typically achieved by sending a signed, but not encrypted, message to Bob.
2. Bob verifies the signature of Alice's certificate by using the CA's public key. If the signature proves to be valid, he accepts the public key in the certificate as Alice's public key. Today's browsers and e-mail programs handle verification automatically.

[1] In cryptographic protocols, the users are often called *Alice* and *Bob*

A.3.6 SmartCards and Readers

SmartCards are credit card-sized devices with integrated circuit chips (ICC) on them. They have their own security mechanisms to lock themselves against physical, electrical and chemical attacks. When private keys are loaded, they never leave the SmartCard and a PIN code protects the key usage. SmartCards are easy to use. They can fit in a wallet and can be easily carried.

Terminals (often called readers, although they are usually able to write as well) are the devices which enable communication between a SmartCard and a computer. Smartcard terminals can be connected to computers via serial or USB ports. An important advantage of some (more expensive) terminals is the secure PIN entry option, which is possible if a reader has its own keypad, display and special software on it.

Figure A.8: SmartCard Terminals

A.3.7 Secure Socket Layer (SSL)

Secure Sockets Layer (SSL), developed by Netscape Communications, is a standard security protocol that provides security and privacy on the web. The protocol allows client/server applications to communicate securely. This is achieved by an online, interactive process which handles secure and authentic exchanges of some random data which is finally used to generate the session key on both sides. SSL uses both public key and session key algorithms. Work flow of the SSL is illustrated in figure A.9. In many cases, client authentication is optional, since clients may not have certificates.

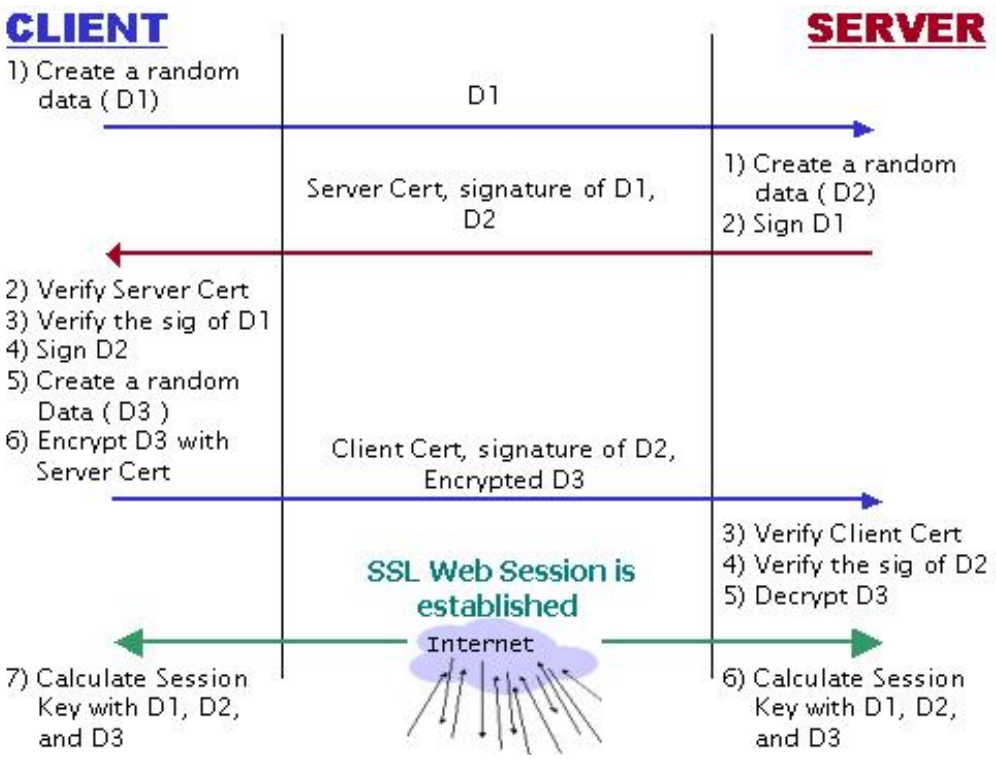
CLIENT
SERVER
1) Create a random data (D1)
D1
1) Create a random data (D2)
2) Sign D1
Server Cert, signature of D1, D2
2) Verify Server Cert
3) Verify the sig of D1
4) Sign D2
5) Create a random Data (D3)
6) Encrypt D3 with Server Cert
Client Cert, signature of D2, Encrypted D3
3) Verify Client Cert
4) Verify the sig of D2
5) Decrypt D3
SSL Web Session is established
Internet
7) Calculate Session Key with D1, D2, and D3
6) Calculate Session Key with D1, D2, and D3

Figure A.9: Secure Socket Layer

A.3.8 Secure Multipurpose Internet Mail Exchange (S/MIME)

Secure Multipurpose Internet Mail Extensions (S/MIME) is an open protocol standard developed by the RSA Laboratories that provides encryption and digital signature functionality to Internet e-mail. S/MIME uses public key cryptography standards to define e-mail security services. S/MIME includes offline processes.

The sender's process is illustrated in figure A.10, the recipient's process is illustrated in figure A.11.

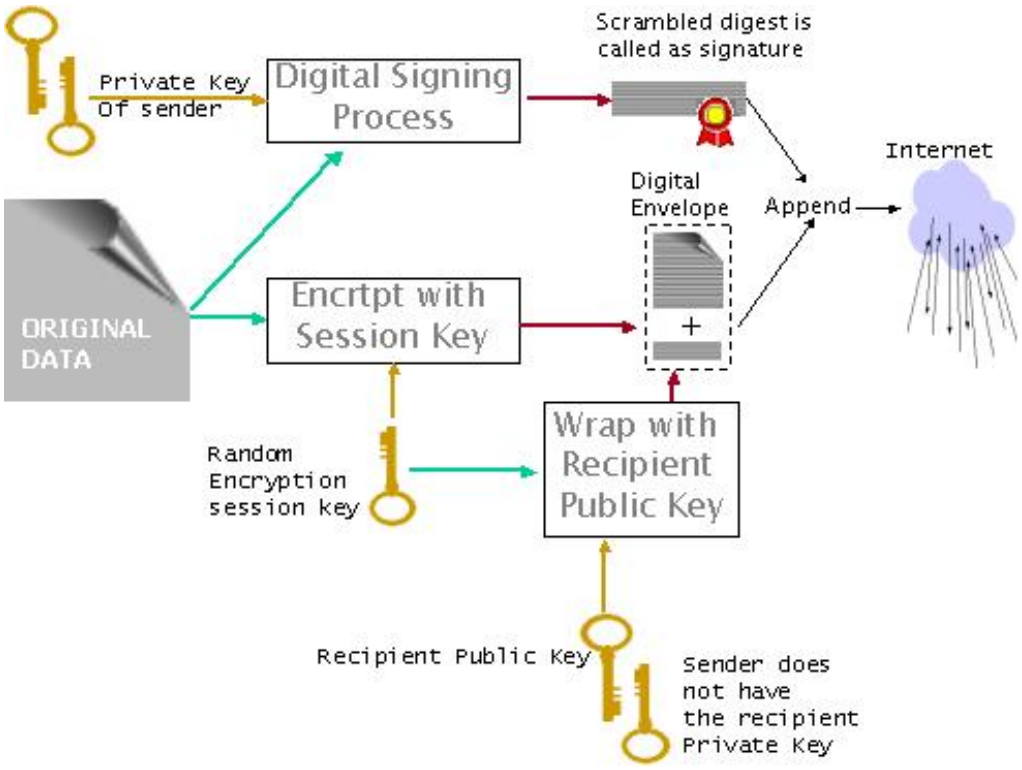

Figure A.10: Sender Process in S/MIME

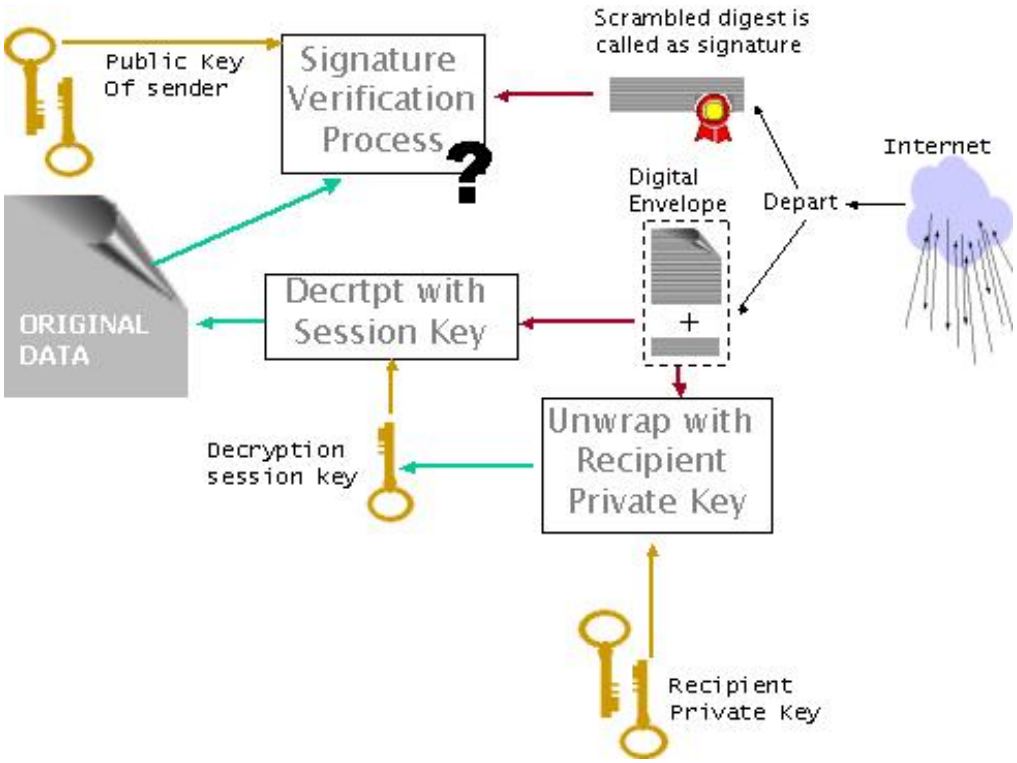

Figure A.11: Recipient Process in S/MIME

Appendix B

Glossary

Algorithm A mathematical formula used to perform computations that can be used for security purposes.

Authenticate To determine the identity of the entity that signed a message (entity authentication), or to verify that a message was not altered (data authentication).

Certificate Authority (CA) An entity with the authority and methods to certify the identity of one or more parties in an exchange (an essential function in public key crypto systems).

Cryptography The art and science of transforming confidential information to make it unreadable to unauthorised parties.

Data Encryption Standard (DES) A block cipher that encrypts data in 64-bit blocks. DES is a symmetric algorithm that uses the same algorithm and key for encryption and decryption. Developed in the early 1970s, DES is also known as the DEA (Data Encryption Algorithm) by ANSI and the DEA-1 by ISO.

Decryption The process in which ciphertext is converted to plaintext.

Digital Certificate A digital certificate provides identification for secure transactions. It consists of a public key and other data about the user, all of which is digitally signed by a Certificate Authority. It is a condition of access to secure e-mail or to secure Web sites.

Digital Signature A data string produced using a public key crypto system to prove the identity of the sender and the integrity of the message.

Encryption A cryptographic procedure whereby a legible message is encrypted and made illegible to all but the holder of the appropriate cryptographic key.

Internet Explorer (IE) Microsoft Internet browser.

Inter-operability The ability of products manufactured by different companies to operate correctly with one another.

Key A value that is used with a cryptographic algorithm to encrypt, decrypt, or sign data. Secret key (symmetric) crypto systems use only one secret key. Public key (asymmetric) crypto systems rely on a matched key pair to encrypt and decrypt data.

Key Length The number of bits forming a key. The longer the key, the more secure the encryption.

MD5 A hashing algorithm that creates a 128-bit hash value, which is twice the size of the block (64 bits).

Personal Computer/Smart Card (PC/SC) Standards that define the interface between smart cards and smart card readers.

Public Key Cryptography Standards (PKCS) A cryptographic system that uses two different keys (public and private) for encrypting data. The most well-known public key algorithm is RSA.

Rivest, Shamir, Adleman (RSA) Developers of the RSA public key crypto system and founders of RSA Data Security, Inc.

Secure Hash Standard (SHA) A standard designed by NIST and NSA. This standard defines the Secure Hash Algorithm (SHA-1) for use with the Digital Signature Standard (DSS).

Secure Sockets Layer (SSL) Security protocol used between servers and browsers for secure Web sessions.

SSL Handshake The SSL handshake, which takes place each time you start a secure Web session, identifies the server. This is automatically performed by your browser.

Secure/Multipurpose Internet Mail Extensions (S/MIME) Standard offline message format for use in secure e-mail applications.

Uniform Resource Locator (URL) Web address.